Open the whistle

GUIDA PRATICA AL WHISTLEBLOWING

Cofinanziato
dall'Unione europea

"*Open the Whistle: Protecting whistleblowers through transparency, cooperation and Open Government strategies*" (OPWHI) è un progetto co-finanziato dall'Unione Europea (Progetto numero: 101140801 — Bando: CERV-2023-CHAR-LITI-WHISTLE) che mira a creare un ambiente favorevole e protetto per le segnalazioni di violazioni del diritto dell'Unione e di altre infrazioni, promuovendo una cultura in cui lə segnalanti possano parlare con sicurezza.

2025 Transparency International España
ISBN: 978-84-09-73335-4

Questo lavoro è distribuito sotto licenza Creative Commons Attribuzione – Non commerciale – Non opere derivate 4.0 Internazionale.

Ideazione grafica e illustrazioni: Alessia Riolo
Design e impaginazione: Álvaro Arribas Jiménez

Cofinanziato dall'Unione europea

Co-finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, allə solə autorə e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

PARTNER DEL PROGETTO

Libera - Associazioni, nomi e numeri contro le mafie - È una rete di organizzazioni della società civile impegnate nella lotta alla corruzione e alla criminalità organizzata e nel contrasto a chi le alimenta, con l'obiettivo di promuovere la giustizia sociale e la democrazia. Fondata in Italia nel 1995, la rete comprende attualmente 278 gruppi locali e 80 organizzazioni internazionali in 35 Paesi in Europa, nei Balcani occidentali, in Africa e in America Latina. Dal 2016 è attivamente impegnata nella tutela delle persone segnalanti, in particolare attraverso Linea Libera, un servizio di ascolto e supporto per potenziali segnalanti sia del settore pubblico che privato. Libera collabora strettamente con l'Autorità Nazionale Anticorruzione (ANAC), le pubbliche amministrazioni, le altre OSC e le comunità locali per supportare al meglio potenziali segnalanti e per promuovere iniziative condivise contro la corruzione.

Università di Pisa (UNIPI) – Dal 2010 il Dipartimento di Scienze Politiche dell'Università di Pisa organizza il Master in "Analisi, prevenzione e contrasto della criminalità organizzata e della corruzione", che ha formato oltre duecento studenti provenienti da tutta Italia e dall'estero sui temi dell'anticorruzione e dell'antimafia. Inoltre, UNIPI gestisce l'Osservatorio sulla Corruzione Politica.

Transparency International Spain[1] **(TI-E**) - Attraverso il monitoraggio delle politiche pubbliche, l'*advocacy*, le campagne di comunicazione e la ricerca, TI-E sostiene una maggiore trasparenza e integrità in tutti i settori della vita pubblica. Per quanto riguarda il settore pubblico, attraverso il dialogo, l'azione collettiva, la formazione e il lavoro congiunto con le pubbliche amministrazioni e il governo, TI-E cerca di promuovere e favorire una cultura di trasparenza, integrità, e responsabilità nel settore pubblico spagnolo. Pertanto, partecipa attivamente alla progettazione, allo sviluppo, al monitoraggio e alla valutazione delle politiche pubbliche in materia di prevenzione della corruzione e di governo aperto, promuove la realizzazione dei principi e degli impegni del governo aperto in Spagna e fa parte di diversi gruppi di *whistleblowing*. Integra una prospettiva di genere in tutte le sue azioni, identificando le disuguaglianze intersezionali e riconoscendo gli impatti differenziati della corruzione e della mancanza di trasparenza.

Center for the Study of Democracy (CSD) - Fondato alla fine del 1989, è un *think-tank* interdisciplinare orientato alla ricerca con focus regionale sull'Europa e sui Paesi dei Balcani occidentali. Il CSD ha pubblicato una serie di rapporti, manuali e guide sulla protezione dei diritti umani, lo Stato di diritto e la lotta alla corruzione. L'organizzazione è attivamente coinvolta nel miglioramento delle politiche e della cultura del *whistleblowing* in qualità di attore regionale anticorruzione e membro della *South East Europe Coalition on Whistleblower Protection* (SECWP). CSD sostiene attivamente il recepimento della Direttiva (UE) 2019/1937 sul *whistleblowing* in Bulgaria. Lə suə espertə hanno partecipato al gruppo di lavoro del Ministero della Giustizia, che ha elaborato la legge di recepimento della Direttiva, e hanno formulato osservazioni su tutti i progetti di legge presentati al parlamento.

[1] *Original name: Transparency international España*

Autorità Nazionale Anticorruzione (ANAC) - È l'autorità italiana preposta al ricevimento e alle indagini sulle segnalazioni di illeciti e sulle comunicazioni di ritorsioni adottate ai danni dellə segnalanti. L'ANAC tutela la riservatezza della loro identità e del contenuto delle segnalazioni e, attraverso l'utilizzo di un sistema di crittografia di una piattaforma informatica, può comunicare in forma anonima con chi segnala. Il potere sanzionatorio dell'ANAC comprende i casi di ritorsione, i casi di inerzia da parte dei soggetti preposti che non hanno effettuato alcuna verifica e analisi della segnalazione ricevuta nonché i casi di mancata o scorretta istituzione di un sistema di gestione delle segnalazioni.

Anti-Fraud Office of Catalonia[2] **(OAC)**.- È un'istituzione di diritto pubblico creata con la legge 14/2008, il 5 novembre dello stesso anno. Il suo scopo è prevenire e indagare su casi di uso o assegnazione illecita di fondi pubblici o qualsiasi altra appropriazione irregolare derivante da atti che comportino un conflitto di interessi o l'uso a vantaggio privato di informazioni derivanti dalle funzioni pubbliche. Fornisce inoltre consulenza e formula raccomandazioni per l'adozione di misure contro la corruzione, le pratiche fraudolente e i comportamenti che violano l'integrità e la trasparenza. All'Ufficio sono state inoltre attribuite le funzioni previste dalla Legge dello Stato n. 2/2023, di recepimento della Direttiva (UE) 2019/1937, che assegna all'Autorità indipendente per la protezione delle persone segnalanti presso l'OAC di esercitare i propri poteri sanzionatori anche in relazione alle violazioni della medesima Legge, che disciplina la tutela dellə segnalanti e la lotta alla corruzione.

Commission for Personal Data Protection[3] **(CPDP)** – La Commissione bulgara per la protezione dei dati personali è l'autorità nazionale incaricata di ricevere le segnalazioni di *whistleblowing*. La CPDP garantisce la protezione delle persone fisiche, tenendo conto delle condizioni, delle procedure e delle misure previste per la tutela dei segnalanti nei settori pubblico e privato, che segnalano o divulgano pubblicamente informazioni riguardanti la legislazione bulgara o atti dell'Unione europea che mettono in pericolo o danneggiano l'interesse pubblico e il diritto dell'Unione.

ITALIA

opengov

Open Government Italia sostiene e promuove la versione italiana di questa guida, riconoscendone il valore in linea con i propri principi, pur non avendo contribuito direttamente alla sua elaborazione o al suo finanziamento.

[2] *Original name: Oficina Antifrau de Catalunya*

[3] *Original name: Komisiya za zashtita na lichnite danni*

RICONOSCIMENTI

I partner del progetto desiderano ringraziare gli inestimabili contributi di tuttə lə espertə, dellə rappresentanti dei partner del progetto e di tuttə coloro che hanno partecipato allo sviluppo di questa guida.

Gruppo di lavoro

ANAC	Giulia Cossu Giovanni Paolo Sellitto Valentina Tomassi
CSD	Maria Yordanova Dimitar Markov
CPDP	Hristo Alaminov Yoan Angelov Atanaska Georgieva Kristina Radkova-Staneva Katya Stanimirova Radostina Takova Desislava Toshkova-Nikolova
Libera	Leonardo Ferrante Elisa Orlando Carlotta Bartolucci
OAC	Elisenda Escoda Marisa Miralles Òscar Roca Jordi Tres
TI-E	David Martínez García Ailén Rubio Arrieta Camila Cella Andrea Rivera
UNIPI	Alberto Vannucci Francesca Rispoli Martina Cataldo Eugenio Pizzimenti

Comitato scientifico del progetto

Laura Valli, ANAC
Massimiliano Andretta, UNIPI
Roberta Bracciale, UNIPI
Valentina Maria Donini, Scuola Nazionale dell'Amministrazione (SNA)
Ventsislav Karadjov, CPDP
Delyana Doseva, CSD
Elisabet Martínez, OAC
Silvina Bacigalupo Saggese, TI-E
Ramón Ragués i Vallès, UPF

SOMMARIO

INTRODUZIONE E STRUTTURA DELLA GUIDA	PG. 7
CAPITOLO 1: TRASPARENZA E COMUNICAZIONE DEI SISTEMI DI SEGNALAZIONE	PG. 14
CAPITOLO 2: CORRETTEZZA DELLE INDAGINI E DELLA GESTIONE NELL'AMBITO DEI SISTEMI INTERNI DI SEGNALAZIONE	PG. 36
CAPITOLO 3: PROTEZIONE DEI DATI PERSONALI	PG. 58
CAPITOLO 4: PROTEZIONE E SOSTEGNO DELLƎ SEGNALANTI	PG. 79
CAPITOLO 5: VALUTAZIONE DELL'EFFICACIA DEL SISTEMA DI SEGNALAZIONE E DELLO SVILUPPO DI UNA CULTURA DEL WHISTLEBLOWING	PG. 97
CAPITOLO 6: RACCOMANDAZIONI SU GENERE E GOVERNO APERTO	PG. 113
OLTRE QUESTA GUIDA	PG. 116

INTRODUZIONE E STRUTTURA DELLA GUIDA

QUAL È LO SCOPO DI QUESTA GUIDA?

Questa guida pratica è un prodotto collettivo frutto della **conoscenza**, della **ricerca** e dell'**esperienza** congiunta di **autorità** e organizzazioni della **società civile** di **Italia**, **Bulgaria** e **Spagna**, con il coordinamento e la guida del mondo accademico, **sul tema del *whistleblowing***.

A partire da questi tre contesti, che certo non esauriscono il quadro ma aiutano a mettere a fuoco alcune principali sfide aperte, offre conoscenze teoriche e orientamenti pratici che hanno, come obiettivo di fondo, il costruire una **nuova narrazione** e un modello solido di protezione delle persone segnalanti. Il fine più immediato è offrire spunti concreti e raccomandazioni operative per implementare le pratiche esistenti, contribuendo a generare **un ambiente sicuro e favorevole** alla segnalazione **e rendere più efficace l'emersione di comportamenti illeciti.**

In queste pagine, esploreremo **cinque sfide** che, a oggi, consideriamo essenziali nel contesto del *whistleblowing*. A ciascuna di esse è dedicato un capitolo della guida:

A. Capitolo 1 → Trasparenza e comunicazione dei sistemi di segnalazione.
B. Capitolo 2 → Correttezza delle indagini e della gestione nell'ambito dei sistemi interni di segnalazione.
C. Capitolo 3 → Protezione dei dati personali.
D. Capitolo 4 → Protezione e sostegno dellə segnalanti.
E. Capitolo 5 → Valutazione dell'efficacia del sistema di segnalazione e dello sviluppo di una cultura del *whistleblowing*.

Dotando le diverse parti interessate degli strumenti e delle conoscenze adeguate, questa guida pratica:

A. Fornisce informazioni sui **meccanismi di segnalazione**, sulle **misure di riservatezza e sulle politiche anti-ritorsione**.
B. Affronta le già dette sfide all'interno delle legislazioni nazionali (la presente traduzione in italiano valorizza **specialmente il contesto della Penisola**) in materia di *whistleblowing* e le questioni derivanti dal **recepimento della Direttiva (UE) 2019/1937 (di seguito, "la Direttiva")** cercando di colmare le lacune esistenti o, ove non possibile, riconoscendo le questioni irrisolte.
C. Fornisce un'**analisi dinamica**, una sorta di fotografia in movimento non esaustiva, esaminando come si sono evolute le misure adottate in risposta alla Direttiva e individuando le sfide ancora aperte **a sei anni dalla sua adozione**.
D. Offre **suggerimenti concreti basati sulle lezioni apprese durante**

questo periodo, con l'obiettivo di informare i miglioramenti futuri.

Inoltre, la guida raccomanda, se non le migliori, almeno **buone pratiche utili a coordinare l'istituto del *whistleblowing* con altre azioni atte a promuovere una cultura della trasparenza, della rendicontabilità al pubblico (*accountability*) e della responsabilità etica**, rafforzando in ultima analisi le istituzioni e aumentando la fiducia della cittadinanza.

QUESTA GUIDA NON È:

A. **Un manuale**: non offre analisi approfondite della Direttiva (UE) 2019/1937 o valutazioni complete per singolo Paese, e non serve come strumento di verifica per valutare la conformità, attraverso l'assegnazione di un punteggio. Non è nemmeno un testo introduttivo all'istituto pensato per un pubblico neofita o per chi intende segnalare, poiché alcune nozioni sono date per acquisite e si rimanda ad altre risorse per eventuali approfondimenti.
B. **Un documento mono-prospettico**: non esamina il whistleblowing esclusivamente da un unico punto di vista, sia esso giuridico, politico o economico. Al contrario, integra più discipline e approcci al fine di fornire una comprensione completa, riconoscendo la natura sfaccettata del whistleblowing.
C. **Un'analisi storica o teorica**: evita di approfondire la storia o i fondamenti teorici del whistleblowing, concentrandosi invece su intuizioni pratiche e raccomandazioni operative.
D. **Una visione unilaterale**: non si concentra solo sulla funzionalità del sistema o esclusivamente sulla protezione delle persone segnalanti, ma riconosce l'importanza di entrambe le prospettive e cerca di armonizzarle.

FOCUS SU DUE APPROCCI TRASVERSALI: GENERE E GOVERNO APERTO

Questa guida utilizza,nell'analisi dei vari argomenti, due prospettive innovative: quella di **genere** e quella del **governo aperto**.

A. **L' approccio di genere** mira a promuovere sistemi di *whistleblowing* **accessibili, inclusivi e attenti alle differenze e alle dimensioni di genere,** per garantire un sistema di segnalazione e una relativa protezione più efficaci e complete. Negli ultimi anni sta crescendo la consapevolezza di come la corruzione, così come la malamministrazione, possa avere un impatto sproporzionato su donne, uomini che lavorano in determinati settori e persone con identità di genere non conformi, a causa di discriminazioni strutturali che ne amplificano i danni. Ciò rende necessario progettare meccanismi di *whistleblowing* che tengano conto di tali differenze, assicurando una protezione adeguata per tutti i gruppi coinvolti. Integrare una prospettiva di genere aiuta a **colmare le lacune esistenti nelle tutele legali e nelle politiche** (pubbliche o d'impresa) che spesso restano cieche rispetto alla diversità, all'uguaglianza e alla non discriminazione.

In questo quadro, la guida intende **fornire strumenti, sia teorici che pratici,** a tutte le parti coinvolte nel *whistleblowing*, facilitando l'effettiva integrazione di un approccio di genere.

- **L'adozione dell'approccio di governo aperto** (***Open Government***) si propone di formulare raccomandazioni utili ad affrontare le sfide del *whistleblowing* sulla base dei principi fondamentali di tale modello di *governance*: **trasparenza** (ove sensata, nel caso del *whistleblowing*), ***accountability*, partecipazione e l'inclusione di differenti *stakeholder* ponendoli sullo stesso piano, valutazione condivisa**. In altre parole, questo testo suggerisce azioni e iniziative che società civile e istituzioni possono intraprendere collettivamente e in modo collaborativo, per favorire il *whistleblowing* e proteggere chi segnala. In questa guida, vogliamo **fornire indicazioni** principalmente a quei Paesi (come lo è l'**Italia**) che sono **membri dell'iniziativa internazionale *Open Government Partnership* (OGP).** Suggeriamo infatti a OGP di farsi carico delle proposte qui formulate, sia includendole nei cicli dei cosiddetti Piani d'Azione Nazionali (*National Action Plan* – NAP[4]), sia prevedendole come singole sfide per il governo aperto (*Open Government Challenge*[5], le quali consentono di assumere e riconoscere impegni di riforma ambiziosi al di fuori del normale ciclo del Piano d'Azione). In questo modo, sarà più semplice auto-vincolarsi al rispetto degli impegni assunti, stabilire un rapporto trasparente con tutte le parti interessate, co-creare soluzioni e monitorarne l'attuazione e l'impatto. Nei Paesi che non aderiscono formalmente all'*Open Government Partnership*, è comunque possibile intraprendere azioni di governo aperto ispirate ai suggerimenti contenuti in queste pagine.

PERCHÉ IL WHISTLEBLOWING È CRUCIALE? LA NECESSITÀ DI RENDERLO UNA COMPONENTE ESSENZIALE E SISTEMICA DELLA SOCIETÀ

Whistleblowing è un termine che racchiude in sé molteplici significati e sfumature. In senso lato, si tratta di una **forma di segnalazione** che svolge un ruolo cruciale nel garantire l'accertamento delle responsabilità, nell'esporre **pratiche scorrette e corruzione,** nel portare alla luce illeciti nascosti e nel prevenirne i relativi danni. Chi segnala ha assistito a illeciti nel proprio ambiente di lavoro o sospetta ragionevolmente il loro verificarsi e, agendo nell'interesse pubblico, ha diritto alla protezione della propria identità e da ritorsioni. Tuttavia, affinché il *whistleblowing* sia veramente efficace, deve essere integrato come **componente essenziale e sistemica** all'interno dei luoghi di lavoro e della società.

Forti tutele legali, meccanismi di segnalazione chiari e una cultura che promuova la responsabilità etica sono fondamentali per consentire alle persone di utilizzare l'istituto senza timore di ritorsioni. Attualmente, le normative comportamentali nelle organizzazioni pubbliche o private e nella società, assieme a una certa conflittualità tra leggi esistenti che ancora permane in tutti e tre i Paesi analizzati, possono scoraggiare le persone dal

[4] *Si veda: https://www.opengovpartnership.org/process/action-plan-cycle/*

[5] *Si veda: https://www.opengovpartnership.org/the-open-gov-challenge/open-government-challenge-areas/*

segnalare illeciti o violazioni etiche. Prevalgono la necessità di adattamento, la percezione di chi segnala come spia o traditore e l'idea che il *whistleblowing* sia una "*extrema ratio*" che richiede enormi sforzi legali. Questo è problematico perché, invece di essere considerato un elemento strutturale di qualsiasi organizzazione e modello organizzativo, pubblico o privato, è ancora visto come una misura straordinaria che richiede interventi eccezionali. Istituzionalizzando il *whistleblowing* come pratica fondamentale, possiamo creare viceversa un ambiente più sicuro, trasparente e responsabile per chiunque.

DUE PROSPETTIVE DIVERSE MA COMPLEMENTARI

Questa guida cerca di bilanciare **due prospettive:**

A. L'approccio "**incentrato sul *whistleblowing***" (*whistleblowing-centred*). Questo punto di vista è principalmente rappresentato dalle autorità competenti, le quali sono più direttamente interessate (ma non esclusivamente) al funzionamento dell'istituto in sé. Secondo tale prospettiva, l'accento è posto sulla gestione del processo di segnalazione, sull'efficacia delle misure di protezione e sull'effettiva applicazione delle normative, quindi sul funzionamento del sistema nel suo complesso, mirando a garantire che le segnalazioni vengano trattate con la dovuta serietà.

B. L' approccio "**orientato al *whistleblower***" (*whistleblower-oriented*). Adottato più frequentemente dalle organizzazioni della società civile, questo approccio pone al centro la persona che segnala, o intende segnalare, o ancora subisce gli effetti di una segnalazione. Qui l'attenzione prioritaria è sulla protezione e sul benessere dellə segnalante, con l'obiettivo di garantire che la persona possa agire senza timore di ritorsioni e che i suoi diritti e progetti di vita siano adeguatamente tutelati. In questo contesto, il focus si sposta dal sistema in sé alla persona che vi interagisce, cercando di assicurare che ogni individuo che prenda la decisione di segnalare sia supportato nel farlo in sicurezza e senza vedere compromessa la propria vita.

BREVE STORIA DELLA DIRETTIVA EUROPEA 2019/1937 E DEL SUO RECEPIMENTO

Nel 2016, la Commissione Europea dichiarò che **non esisteva una base giuridica** per una Direttiva sul *whistleblowing*. Tuttavia, emerse contemporaneamente la necessità di una legislazione armonizzata a livello dell'Unione Europea per garantire la protezione dellə segnalanti su tutto il suolo comunitario, in modo possibilmente uniforme.

Nel 2019, una lunga serie di scandali di alto profilo, come *LuxLeaks* e *Panama Papers*, unita ad altrettanto numerose campagne promosse dalla società civile[6], ha spinto il Parlamento europeo e il Consiglio ad adottare la **Direttiva (UE) 2019/1937.** Il suo scopo era, ed è tuttora, quello di stabilire uno

[6] *Una di queste campagne internazionali, dal nome di Restarting the future, è partita nel 2014 dall'Italia ed è stata condotta da Libera e Associazione Gruppo Abele ONLUS (oggi Fondazione), al fine di chiedere all'Europa proprio una Direttiva sul whistleblowing.*

***standard* minimo per la protezione dellə segnalanti in tutti gli Stati membri dell'UE**, garantendo che le persone che segnalano violazioni del diritto dell'UE siano salvaguardate dalle ritorsioni.

Agli Stati membri dell'UE è stato concesso tempo fino al 17 dicembre 2021 per recepire la Direttiva nel diritto nazionale. Tuttavia, sebbene questo termine fosse vincolante, solo a partire dal 2024 la maggior parte degli Stati membri dell'Unione ha recepito la Direttiva nei propri ordinamenti giuridici. Alcuni Stati, però, hanno incontrato e incontrano ancora oggi difficoltà nel garantire una piena conformità. Le legislazioni nazionali, infatti, variano notevolmente da un Paese all'altro, sia per quanto riguarda le condizioni di protezione delle persone segnalanti sia per la loro base giuridica.

IL *WHISTLEBLOWING* IN ITALIA

In **Italia**, a differenza degli altri Paesi analizzati (in cui le leggi già facevano riferimento al *whistleblowing,* ma in forme più generiche e sparse), **esisteva una normativa specifica dedicata già prima dell'adozione della Direttiva europea**.

Le prime misure sono state introdotte con la Legge 190/2012 e successivamente ampliate nel 2017.

La **Legge 190/2012 sulla prevenzione della corruzione è stata la prima in Italia** a introdurre tutele per chi segnala illeciti, limitatamente, però, al solo settore pubblico. Essa permetteva allə dipendenti del settore pubblico di segnalare comportamenti scorretti di cui venivano a conoscenza senza temere ritorsioni, ma le protezioni erano ancora deboli e il contesto decisamente poco definito. Non c'era infatti un quadro normativo completo e non venivano offerti veri meccanismi di protezione né garanzie per la riservatezza delle segnalazioni. Inoltre, la legislazione non contemplava disposizioni per il settore privato.

Qualche anno dopo, la **Legge 179 del 2017 ha esteso le tutele anche ad alcuni enti del settore privato,** introducendo misure più robuste, tra cui la garanzia di riservatezza delle segnalazioni e l'introduzione di sanzioni contro le ritorsioni.

Oggi, la legge sul *whistleblowing* che traspone la Direttiva europea, ossia il **Decreto legislativo 24/2023**, stabilisce che i soggetti pubblici e privati con più di 50 dipendenti debbano implementare canali interni di segnalazione che ne assicurino la riservatezza. Si dirà in queste pagine di come andiamo conformandoci alla Direttiva nella previsione dei tre canali di segnalazione (cosa precedentemente non prevista), di come oggi si riconosca anche il ruolo delle organizzazioni del terzo settore nel supportare chi segnala o subisce ritorsioni, dell'estensione delle forme di protezione anche a liberə professionistə, volontarə, tirocinanti, azionistə e facilitatorə e altre innovazioni chiave. Nonostante evidenti progressi, però, rimangono ancora numerosi passi da fare e, in alcuni casi, sostanziali criticità, come si dirà in seguito.

IL *WHISTLEBLOWING* IN BULGARIA

Prima dell'adozione della Direttiva europea, la **Bulgaria** già presentava disposizioni disseminate in varie leggi relative alla protezione dellə segnalanti. **La legge sulla protezione contro la discriminazione vietava le ritorsioni** contro le persone che presentavano denunce di discriminazione, mentre il codice di procedura amministrativa offriva garanzie generali per coloro che segnalavano abusi di potere o corruzione. Diversi organismi sono stati coinvolti nella gestione di tali segnalazioni, tra cui l'ispettorato capo del Consiglio dei Ministri, gli ispettorati ministeriali e la Commissione anticorruzione, che fungeva da autorità centrale per la ricezione delle segnalazioni di corruzione e conflitti di interesse. Inoltre, **alcune istituzioni pubbliche e imprese private,** in particolare quelle che operano a livello internazionale o in settori regolamentati, avevano già sviluppato **meccanismi di segnalazione interna.**

Questo quadro frammentato ha contribuito a facilitare il recepimento della Direttiva nel diritto nazionale. **Nel 2023 la Bulgaria ha adottato la legge sulla protezione delle persone che segnalano o divulgano pubblicamente** informazioni sulle violazioni, entrata in vigore il 4 maggio di quell'anno. La legge impone ai datori di lavoro del settore pubblico e privato con 50 o più dipendenti di istituire canali di segnalazione interna, con l'obbligo per i datori di lavoro privati con 50-249 dipendenti a partire dal 17 dicembre 2023. Da allora la Commissione per la protezione dei dati personali (CPDP), designata come canale esterno per le segnalazioni, ha adottato misure importanti per attuare e far rispettare la legislazione.

IL *WHISTLEBLOWING* IN SPAGNA

Ai sensi della legge di procedura penale (***Ley de Enjuiciamiento Criminal* o LECrim**) istituita nel 1882, le persone in **Spagna** che assistono a illeciti sono legalmente obbligate a denunciarli, con sanzioni in caso di inosservanza. Questo obbligo si estende ai cosiddetti "testimoni di riferimento" (LECrim, Art. 264) e ad alcune professioni, come le autorità pubbliche, che sono soggette a pene più severe per la mancata denuncia dei reati (LECrim, Art. 262 e codice penale spagnolo, Art. 408).

D'altra parte, **la riforma del codice penale spagnolo del 2015** ha introdotto il requisito per cui i programmi di *compliance* devono includere l'obbligo di segnalare "possibili rischi e violazioni all'organo responsabile della supervisione del funzionamento e dell'applicazione del modello di prevenzione" (Art. 31 bis 5.4). Sebbene il codice penale non includa questo come obbligo, in caso di processo penale, gli enti che desiderano ottenere un'esenzione o un'attenuazione della loro responsabilità devono disporre di canali interni di *whistleblowing*, il che in pratica ha fatto sì che in **Spagna** molti enti privati (soprattutto grandi aziende) adottassero questi meccanismi prima dell'adozione della Direttiva europea, ciascun soggetto sviluppando le proprie politiche e procedure di protezione dellə segnalanti. Nel settore pubblico, ci sono state anche alcune norme a livello regionale

precedenti alla Direttiva, per esempio **la Legge 11/2016, del 28 novembre**, che istituisce l'Agenzia per la prevenzione e la lotta contro la frode e la corruzione della Comunità Valenzana, che deve stabilire canali riservati che garantiscano la massima riservatezza per la formulazione delle segnalazioni quando lə segnalante invoca l'applicazione dello statuto regolato in questa legge.

Tuttavia, la **Spagna** non disponeva di una protezione diffusa e coerente per lə segnalanti fino al recepimento della **Direttiva del 2019, attuato attraverso la Legge 2/2023, del 20 febbraio,** che disciplina la protezione delle persone che segnalano violazioni normative e la lotta alla corruzione.

Trasparenza e comunicazione dei sistemi di segnalazione

Capitolo 1

Open the whistle

TRASPARENZA E COMUNICAZIONE DEI SISTEMI DI SEGNALAZIONE

CAPITOLO 1

1.1 SISTEMA DI WHISTLEBLOWING: LA NECESSITÀ DI LINEE GUIDA CHIARA

La fiducia[7] nel sistema è un fattore chiave per qualsiasi segnalante. Questa frase è un vero e proprio *mantra* quando si parla di *whistleblowing* e tornerà spesso anche in queste pagine.

Tale fiducia non può fondarsi esclusivamente sull'esistenza di un canale formale atto a raccogliere le segnalazioni: **la mancanza di informazioni** sui canali disponibili e sul funzionamento del sistema può comprometterla seriamente. Garantire piena informazione, trasparenza e comprensibilità è quindi il primo passo imprescindibile per costruire **un ambiente favorevole e protetto**, capace di offrire non solo strumenti, ma anche **condizioni reali di ascolto e tutela**.

L'assenza di linee guida chiare può portare a una disinformazione, scoraggiando chi vuole segnalare e ostacolando la creazione di uno spazio sicuro e affidabile. Pertanto, per aumentare la consapevolezza e la fiducia, **è necessario fornire almeno informazioni su:**

A. Chi può o deve segnalare.
B. Come segnalare.
C. Quando effettuare la segnalazione.
D. A chi effettuare la segnalazione.
E. Come viene tutelata la persona segnalante.
F. Quali sono i diritti della persona segnalata.
G. Come funziona il processo di segnalazione.
H. Le misure di sicurezza in atto.
I. Come garantire che il sistema di segnalazione sia sensibile alla dimensione di genere.

Alcuni dati a sostegno: Secondo una consultazione pubblica europea del 2017, solo il **15% dellə cittadinə comunitarə conosceva le norme** vigenti sulla protezione dellə segnalanti e **il 49% non sapeva a chi rivolgersi** per segnalare casi di corruzione[8]. Allo stesso modo, è dimostrato da numerosi

---

[7] *Secondo Binikos (2008), la fiducia nella propria organizzazione e gestione è stata positivamente associata all'intenzione di segnalare in 16 studi (tra gli altri: Attree, 2007; Brennan e Kelly, 2007; Binikos, 2008; Curtis e Taylor, 2009; Seifert et al., 2014; ecc.).*

[8] *Si veda: https://ec.europa.eu/newsroom/just/items/54254/en*

studi[9] che definire procedure operative chiare o linee guida per lə funzionarə, per il personale delle autorità e per lə segnalanti rappresenta una pratica efficace per incentivare e gestire correttamente le segnalazioni. Poiché il *whistleblowing* è un processo complesso, con numerosi implicazioni, incluso quelle personali e psicologiche, sono necessarie misure organizzative e culturali per supportare l'attuazione della legge, tenendo conto anche degli atteggiamenti culturali nei confronti di chi segnala[10].

Abbiamo scelto di affrontare il tema in questa guida perché, nonostante **la Direttiva** definisca chiaramente i diritti e i principi, è necessario **fornire disposizioni chiare e dettagliate in merito alle informazioni e alla trasparenza che tutti i soggetti obbligati (Art. 8)** devono predisporre sui loro canali e sistemi.

L'Art. 13 della Direttiva stabilisce infatti l'obbligo generale per le autorità competenti di garantire massima informazione e trasparenza circa l'istituto, mentre l'Art. 9, Par. 1, impone ai soggetti obbligati il vincolo di informare in merito alle "procedure per la segnalazione esterna alle autorità competenti ai sensi dell'Art. 10 e, se del caso, alle istituzioni, agli organi o agli organismi dell'Unione" (Art. 9, Par. 1).

Chi intende segnalare potrebbe non avere adeguatamente informazione sui canali disponibili, sul sistema di segnalazione, sulle procedure e le autorità coinvolte, sui diritti, sulle scadenze, sulle informazioni tecniche, sulle misure di protezione e sulle caratteristiche del sistema di sicurezza informatica.

In **Italia**, **tutti i soggetti pubblici e privati sono tenuti a fornire informazioni chiare sul canale, sulle procedure e sulle condizioni** per effettuare sia le segnalazioni interne che quelle esterne[11]. Queste informazioni devono essere facilmente visibili sul posto di lavoro e accessibili alle persone che hanno un rapporto giuridico con l'ente. Se l'ente ha un sito *web*, le informazioni devono essere pubblicate in una sezione specificatamente predisposta. Inoltre, la legge[12] stabilisce che, in qualità di autorità competente per la gestione del canale di segnalazione esterna e

---

[9] *Commissione australiana per i titoli e gli investimenti, 2023; tra gli altri.*

[10] *Teichmann et al., 2022. chi riveli o diffonda informazioni sulle violazioni:*

coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o

relative alla tutela del diritto d'autore o

alla protezione dei dati personali ovvero

se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.chi riveli o diffonda informazioni sulle violazioni:

coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o

relative alla tutela del diritto d'autore o

alla protezione dei dati personali ovvero

se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.

[11] *Art.5.1 D.L., 24/2023 del 10 marzo*

[12] *Art. 9, D.Lgs. 24/2023, di recepimento della Direttiva (UE) 2019/1937*

garante del funzionamento dell'intero istituto, l'ANAC (per come già avviene[13]) deve pubblicare informazioni quali:

A. Misure di protezione per lə segnalanti.
B. Dati di contatto, quali il numero di telefono dell'ufficio che gestisce le segnalazioni, con l'indicazione se le conversazioni telefoniche sono registrate o meno, l'indirizzo postale e l'indirizzo di posta elettronica, sia ordinaria che certificata.
C. Le norme di riservatezza applicabili ai rapporti esterni e interni.

In **Spagna**, la Legge 2/2023[14] del 20 febbraio, che regola la protezione delle persone che segnalano violazioni normative e la lotta alla corruzione, dedica il Titolo IV alla regolamentazione delle informazioni che devono essere fornite sia dagli enti che dalle autorità competenti sui canali interni ed esterni. **La legge prevede espressamente che queste informazioni debbano essere visibili su siti *web*** o piattaforme elettroniche, in una sezione separata e facilmente accessibile. Richiede inoltre che tutti i soggetti tenuti a disporre di un canale interno, sia nel settore pubblico che in quello privato, debbano tenere un registro dei reclami ricevuti e delle eventuali indagini interne che ne derivano. Tuttavia, questo registro non è pubblico ed è accessibile solo alle autorità giudiziarie.

La Legge 2/23 Art. 25 stabilisce esplicitamente che "i soggetti inclusi nell'ambito di applicazione della legge devono fornire adeguate informazioni, in forma chiara e facilmente accessibile, sull'uso di qualsiasi canale interno di segnalazione da essi implementato, nonché sui principi essenziali della procedura di gestione. Nel caso in cui si disponga di un sito *web*, tali informazioni devono essere inserite nella pagina principale (*home page*), in una sezione separata e facilmente identificabile". **Tuttavia, la legge non specifica il contenuto essenziale** di ciò che gli enti devono necessariamente informare al pubblico sui loro sistemi di segnalazione nei loro siti *web*[15].

In **Bulgaria**, la legge sulla protezione delle persone che segnalano o divulgano pubblicamente informazioni sulle violazioni del 4 maggio 2023, in linea con la Direttiva, stabilisce che "(...) **I soggetti obbligati forniscono informazioni chiare e facilmente accessibili** sulle condizioni e sulle procedure per la presentazione delle segnalazioni di irregolarità. Le informazioni sono messe a disposizione sui siti *web* dei soggetti obbligati e in luoghi ben visibili negli uffici e nei luoghi di lavoro"[16] (Art. 12, Par. 4).

---

[13] *Si veda: https://www.anticorruzione.it/-/whistleblowing*

[14] *Si veda: https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513*

[15] *Per le autorità di cui all'Art. 24, la legge fa un po' più di chiarezza, stabilendo che esse devono pubblicare, in una sezione separata, facilmente identificabile e accessibile del loro sito web, almeno le seguenti informazioni: "a) le condizioni per l'ammissibilità alla protezione ai sensi della presente legge; b) i dati di contatto dei canali di informazione esterna di cui al titolo III, in particolare gli indirizzi di posta e di posta elettronica e i numeri di telefono associati a tali canali, con l'indicazione della registrazione delle conversazioni telefoniche; c) le procedure di gestione, compreso il modo in cui l'autorità competente può chiedere alla persona segnalante di chiarire le informazioni comunicate o di fornire informazioni supplementari, l'eventuale termine per la risposta al segnalante e il tipo e il contenuto di tale risposta; d) Il regime di riservatezza applicabile alle comunicazioni e, in particolare, alle informazioni sul trattamento dei dati personali in conformità con le disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, della Legge Organica 3/2018 del 5 dicembre e del Titolo VII di tale legge. e) i rimedi e le procedure per la protezione contro le ritorsioni e la disponibilità di consulenza riservata. In particolare, sono previste le condizioni per l'esonero dalla responsabilità e l'attenuazione della sanzione di cui all'articolo 40 e f) i recapiti dell'Autorità indipendente per la protezione dellə segnalanti, I.W.P.A. o dell'autorità o dell'organismo competente interessato".*

[16] *Legge sulla protezione delle persone che segnalano o divulgano pubblicamente informazioni sulle violazioni, Bulgaria, 4 maggio 2023, articolo 12, paragrafo 4*

Sebbene tale obbligo sia stato formalmente attuato, **non vi è alcuna valutazione della sua efficacia** (cfr. **capitolo 5**)

Cp. 5 >

Lo ripetiamo ancora una volta: trasparenza e comunicazione efficace non sono questioni secondarie, ma sono essenziali per garantire il corretto funzionamento dei sistemi di *whistleblowing*. **Le persone non possono decidere consapevolmente se, quando e come effettuare la segnalazione se non sono adeguatamente informate** in anticipo sui loro diritti e obblighi fondamentali, sui principi e le fasi essenziali del processo di segnalazione e sui dettagli di base sulla natura e sul funzionamento dei canali di segnalazione all'interno di un'organizzazione o di un ente pubblico[17].

Inoltre, **le autorità e gli organi di vigilanza possono vigilare più facilmente sulle parti obbligate all'implementazione di canali di segnalazione,** monitorando il rispetto attraverso revisioni periodiche della loro trasparenza e accessibilità.

Dalla lettura attenta della Direttiva (i Considerando numero 59 e numero 75), dell'Art. 25 della legge spagnola 2/23, l'Art. 12 della legge bulgara sulla protezione dellə segnalanti, gli Artt. 5.1 e 9.1 del D.L. italiano 24/2023, e alla luce di quanto detto finora, consegue che devono essere soddisfatte **due condizioni fondamentali** per garantire un'adeguata e completa trasparenza nei sistemi e nei canali di segnalazione in modo che possano adempiere efficacemente alla loro missione: uno relativo al **contenuto** e un altro relativo alla **forma**.

Con **"contenuto" ci riferiamo alle informazioni che devono essere fornite**. Le persone devono sapere cosa è accettabile segnalare, quali diritti hanno come segnalanti, come viene gestita la loro segnalazione, e come vengono tutelate da eventuali ritorsioni.

Con **"forma", ci riferiamo al modo in cui queste informazioni vengono comunicate**. Non basta che ci siano delle informazioni, ma devono essere presentate in un formato che sia facilmente comprensibile, accessibile e adeguato alle esigenze delle persone che potrebbero dover segnalare. Questo potrebbe includere la chiarezza delle istruzioni, la disponibilità dei canali di segnalazione, e la facilità con cui un individuo può accedere a queste informazioni.

Segue un dettaglio su entrambe queste condizioni.

---

[17] *Il legislatore europeo è stato molto chiaro al riguardo: "Tutti i soggetti che stanno valutando la possibilità di segnalare violazioni del diritto dell'Unione dovrebbero essere in grado di prendere una decisione informata su se, quando e come effettuare la segnalazione. I soggetti giuridici del settore pubblico e privato che dispongono di procedure di segnalazione interna dovrebbero fornire informazioni su tali procedure, nonché sulle procedure di segnalazione esterna alle autorità competenti. È essenziale che queste informazioni siano chiare e facilmente accessibili, anche, per quanto possibile, a soggetti che non sono dipendenti in contatto con l'ente in ragione della loro attività professionale, come fornitori di servizi, distributori, fornitori e partner commerciali. Ad esempio, tali informazioni potrebbero essere visualizzate in un luogo visibile accessibile a tutti questi individui e sul sito web dell'ente, e potrebbero anche essere incluse in corsi di formazione e seminari in materia di etica e integrità". (Considerando 59 della Direttiva (UE) 2019/1937). Inoltre, in un successivo considerando, si ribadisce che "tutte le informazioni relative alle segnalazioni devono essere trasparenti, facilmente comprensibili e affidabili al fine di incoraggiare la segnalazione piuttosto che ostacolarla". (Considerando 75 della Direttiva (UE) 2019/1937).*

1.2 TRASPARENZA IN MERITO AI DIRITTI E ALLE GARANZIE DELLƎ SEGNALANTI E DELLƎ SEGNALATƎ

Per quanto riguarda l'aspetto di contenuto, come detto tutte le parti obbligate devono fornire informazioni almeno sui seguenti ambiti:

1.2.1 TRASPARENZA IN MERITO AI DIRITTI E ALLE GARANZIE DELLE PERSONE SIA SEGNALANTI CHE SEGNALATE

Intendiamo sottolineare, in questa guida, come sia **necessario inserire una sezione specifica sul sito *web* che con un elenco completo dei diritti sia dellə segnalanti che dellə segnalatə**, nonché di terzi (per esempio qualcunə che è menzionato nella segnalazione, testimoni, rappresentanti/ sindacati dei lavoratori, collaboratorə della persona segnalante) se applicabile.

Per quanto riguarda lə potenziali segnalanti, tale elenco dovrebbe includere almeno:

A. Tutela della riservatezza di chi segnala e del contenuto della segnalazione.
B. Divieto di ritorsione[18] nei termini stabiliti dalla Direttiva e dalle leggi nazionali.
C. Informazioni chiare sugli enti che gestiscono la segnalazione.
D. Ricezione di una risposta motivata sulla decisione di archiviare, respingere o non procedere con la segnalazione.
E. Protezione dei dati personali.[19]
F. Conferma di ricezione e attento seguito delle segnalazioni.
G. Notifica di risoluzione tempestiva e appropriata.[20]
H. Un'indagine equa, indipendente e imparziale.
I. Consulenza legale, sostegno giuridico e psicologico o supporto da parte dellə rappresentanti dellə lavoratorə (se richiesto dalla legge).
J. Diritto a una buona amministrazione, ai sensi dell'Art. 41 della Carta dei diritti fondamentali dell'Unione europea (particolarmente rilevante per i soggetti obbligati del settore pubblico).
K. Supporto psicologico (se richiesto dalla legge od offerto dall'ente).
L. Sostegno finanziario (se richiesto dalla legge od offerto dall'ente).

Per quanto riguarda le parti destinatarie della segnalazione, ossia le persone segnalate, è necessario includere almeno:

A. Presunzione di innocenza.
B. Tutela dell'identità/riservatezza.

---

[18] *Secondo uno degli esperti intervistati, è importante riferire su come vengono prevenute le ritorsioni, su come viene garantita la protezione dellə segnalanti e delineare i processi specifici che lo garantiscono.*

[19] *Inclusi, a titolo esemplificativo ma non esaustivo: il diritto di essere informato sull'identità del titolare del trattamento, lo scopo del trattamento e la possibilità di esercitare i diritti di cui agli Artt. da 15 a 22 del RGPD e il diritto alla cancellazione dei dati dopo tre mesi, a meno che non siano disciplinari o penali o procedimenti penali.*

[20] *A tal proposito, si veda: Indicatore n. 94 del Rapporto TRAC-SPAGNA 2022 (p. 159).*

- Diritto al giusto processo (che si declina, tra l'altro, nel diritto di ricevere ascolto, nel diritto di accesso al fascicolo dell'indagine, nel diritto di presentare prove e di conoscere l'organo inquirente nonché nel diritto a un giudice imparziale)
- Diritti in materia di protezione dei dati personali.

Infine, è anche **cruciale includere i diritti e le garanzie di terzi potenzialmente collegati, colpiti o nominati in una segnalazione** (testimoni, persone nominate in una segnalazione, familiari o persone che potrebbero subire qualche tipo di danno o ritorsione a seguito della segnalazione, nonché coloro che forniscono supporto legale, lavorativo o psicologico). e dovrebbero essere inclusə anche facilitatorə e i centri di informazione (cfr. **capitolo 4** per ulteriori dettagli su quali siano le forme di tutela previste per queste figure).

Cp. 4>

1.2.2 Trasparenza sull'ambito di applicazione materiale.

In questa guida suggeriamo vivamente di **indicare quali illeciti o atti di malamministrazione possono essere segnalati (ossia cosa va segnalato), nonché le normative applicabili**[21], adattandole alle peculiarità dell'ente di riferimento (pubblico o privato) ed evitando riferimenti generici o astratti. Inoltre, raccomandiamo che i canali interni ed esterni forniscano un punto di contatto per le richieste e una **sezione di domande frequenti (*Frequently Asked Questions,* FAQ).**

A riguardo, va però tenuto in conto che tutte lə espertə in ambito giuridico intervistatə nei tre Paesi analizzati hanno evidenziato come **le leggi di recepimento abbiano lasciato ambiguità, disuguaglianze o aree non protette riguardo alla definizione di ciò che può o non può essere segnalato**. Tali lacune possono scoraggiare lə potenziali segnalanti. Per esempio, la Legge 2/2023 in **Spagna** esclude dalla protezione legale lə segnalanti che riportano irregolarità legate a reati minori non contemplati dalla Direttiva. In **Italia**, almeno teoricamente e per come si vedrà (cfr. capitolo 4.3), l'interpretazione è differente.

Un intervento del legislatore europeo volto a colmare queste lacune è auspicabile.

[21] *Anche un altro dei nostri intervistati ha sottolineato che è fondamentale essere informati sul quadro giuridico e sul rischio di contenzioso.*

FOCUS GENERE

Le parti interessate di tutti i settori e Paesi sottolineano la necessità di affrontare **le disuguaglianze intersettoriali e intersezionali**, l'integrazione di genere e gli approcci alla diversità. La natura della cattiva condotta segnalata, così come il rischio associato, influiscono in modo significativo sulla decisione di segnalare.

I casi di abusi di potere basati sul genere, come le molestie sessuali o la *sextortion*, sono spesso collegati a un rischio più elevato di ritorsioni (cfr. **capitolo 4**), che può scoraggiare le vittime dal denunciare. In alcuni casi, le vittime possono non essere sicure che tale cattiva condotta rientri nella legislazione sul *whistleblowing*. Le parti interessate hanno raccomandato di includere esplicitamente queste questioni nell'ambito di applicazione del *whistleblowing*. In Bulgaria, lə rappresentanti della società civile hanno sottolineato che, se sorgono questioni di genere sul luogo di lavoro, la legislazione in materia di *whistleblowing* dovrebbe affrontarle insieme alle disposizioni giuridiche esistenti contro la discriminazione.

Cp. 4>

Si consiglia di:

A. Garantire che la legislazione dell'UE in materia di violenza di genere e le norme nazionali siano integrate nei meccanismi di segnalazione delle irregolarità per fornire una protezione completa. Ampliare l'ambito della protezione per coprire tutti i potenziali illeciti, abusi e altri reati, comprese le molestie sessuali e la *sextortion*. Il quadro giuridico in materia di segnalazione di irregolarità dovrebbe affrontare la discriminazione di genere sul luogo di lavoro, in aggiunta alle disposizioni giuridiche applicabili contro la discriminazione, e fornire sostegno e protezione alle vittime di *sextortion* e molestie sessuali nell'ambito della legislazione in materia di *whistleblowing*.

B. I futuri quadri normativi internazionali, nazionali e subnazionali dovrebbero rafforzare le misure volte a stabilire meccanismi di protezione su misura per le donne segnalanti e altri gruppi vulnerabili, garantendo che i canali di segnalazione siano accessibili, inclusivi e rispondenti alle loro esigenze e ai loro rischi specifici.

C. Sviluppare protocolli sensibili alle questioni di genere nel quadro legislativo sul *whistleblowing* per affrontare in modo specifico i casi di molestie sessuali, *sextortion* e altri comportamenti scorretti basati sul genere. Integrare la trasparenza in merito ai diritti e alle tutele dellə segnalante con particolare attenzione alla comunicazione sensibile al genere e all'inclusione dei gruppi emarginati. Una comunicazione chiara sui diritti, le garanzie e le autorità responsabili della gestione delle segnalazioni assicura che lə segnalanti si sentano sicurə nel sistema e comprendano le loro protezioni. Ciò include linee guida chiare e accessibili sulle procedure, le opzioni di supporto e le tutele legali contro le ritorsioni.

D. Coordinarsi con altri servizi per una gestione più efficace e prevenire l'impunità, evitando di dare per scontato che i casi di *sextortion* possano essere affrontati meglio da altri servizi o meccanismi di denuncia, come quelli che si occupano di violenza sessuale.

E. Fornire esempi concreti di casi basati sul genere per migliorare la chiarezza e l'accessibilità per potenziali segnalanti, rafforzando i loro diritti e le tutele disponibili.

F. Ogni persona dovrebbe essere informata del proprio diritto di denunciare o divulgare illeciti direttamente alle autorità specializzate competenti, come la polizia, la procura o i tribunali, in particolare nei casi di violenza di genere. Ciò garantisce che la persona sia a conoscenza di tutte le opzioni disponibili per affrontare il problema e cercare il supporto appropriato. Gli accordi di risarcimento non dovrebbero escludere l'accesso ai sistemi giudiziari.

G. Garantire che le piattaforme di segnalazione utilizzino un linguaggio chiaro e non tecnico e offrano canali in più lingue, tra cui la lingua dei segni e altri formati accessibili, per accogliere una gamma diversificata di segnalanti. Garantire un linguaggio inclusivo di genere, rendendo visibile il genere quando pertinente ed evitando inutili marcatori di genere quando non pertinenti alla segnalazione. Questo approccio promuove la chiarezza, l'inclusività e il rispetto delle diverse identità di genere in tutte le forme di comunicazione.

H. Considerare l'impatto delle disparità di accesso digitale, garantendo meccanismi alternativi di segnalazione *offline* per le persone che non dispongono di un accesso sicuro a *internet*, promuovendo l'inclusività per tuttə lə utenti indipendentemente dalle loro capacità di accesso digitale.

QUALE APPROCCIO DI GENERE NELLE NORMATIVE DI RECEPIMENTO?

ITALIA

In Italia, **il concetto di molestie sessuali è rilevante dal punto di vista della legge antidiscriminazione**. Nel 2006 l'Italia ha adottato il cosiddetto "Codice per le pari opportunità tra uomini e donne" (D.L. 198/2006), che contiene una definizione di molestie sessuali. Poiché la legislazione in materia di *whistleblowing* non copre le molestie sessuali sul lavoro, è lasciata alla volontà dei datori di lavoro l'implementazione di procedure interne che consentano allə dipendenti di segnalare molestie o bullismo.

SPAGNA

In Spagna, la Legge 2/2023 non affronta esplicitamente la violenza di genere. Tuttavia, **opera all'interno di un quadro normativo riconosciuto per la prevenzione della violenza di genere, l'uguaglianza e la non discriminazione**, nonché di piani nazionali e politiche pubbliche specifiche su questo tema. Tre i punti chiave che meritano di essere menzionati:

A. L'ambito di applicazione materiale della legge va oltre i requisiti europei e si applica sia ai reati penali che a quelli amministrativi, comprese le violazioni del diritto nazionale. Ciò consente ai meccanismi di segnalazione di affrontare tutti i reati di violenza di genere.
B. Anche se la legge non preclude l'inserimento di questo tema in regolamenti o protocolli, la protezione di genere è pienamente compatibile con il quadro giuridico del *whistleblowing*. Non solo entrambi dovrebbero essere integrati con il quadro giuridico della violenza di genere, ma la legge sul *whistleblowing* include anche tutele per lə lavoratorə che segnalano qualsiasi forma di abuso o violazione della loro dignità, salute e sicurezza. Pertanto, la protezione e le garanzie devono riguardare qualsiasi violazione dell'integrità fisica o psicologica, compresa qualsiasi forma di discriminazione di genere o abuso sessuale.
C. Il Regio Decreto che istituisce l'Autorità Indipendente per la Protezione dellə Segnalanti (A.A.I.) impone una rappresentanza equilibrata di genere all'interno della Commissione Consultiva, stabilendo un prezioso precedente per altre autorità nazionali o locali.

BULGARIA

In Bulgaria le molestie sessuali non sono coperte dalla legge nazionale sul *whistleblowing*. Tuttavia, si ritiene che se le molestie si verifichino in un contesto lavorativo e minaccino l'interesse pubblico, **la segnalazione potrebbe essere considerata una denuncia di irregolarità** e allə segnalante potrebbe essere concessa la dovuta protezione.

1.2.3 Trasparenza in merito ai principi essenziali della procedura di gestione.

Sempre rimanendo in ambito di trasparenza circa il "contenuto", gli enti coinvolti devono **definire e comunicare chiaramente i principi essenziali[22] della procedura di *whistleblowing*, compresi lo scopo, la gestione e il quadro di conformità.** Fornire informazioni adeguate in questa sezione è fondamentale per informare sul motivo dell'esistenza del canale di segnalazione, incoraggiare l'uso corretto del sistema e scoraggiare l'uso improprio.

A. Per quanto riguarda **la sicurezza**, è essenziale informare sulle caratteristiche informatiche del *server* o della piattaforma e sulle misure di sicurezza delle informazioni in atto per garantire un ambiente digitale sicuro per segnalanti, vale a dire: crittografia, pseudonimizzazione, codifica, scatole nere, controllo degli accessi, protocolli di connessione sicura, autenticazione in due fasi, regole di convalida, descrizioni appropriate dei *firewall*, descrizioni complete delle caratteristiche del *server/software, Token CSRF*, ecc.

B. Per quanto riguarda **la protezione da ritorsioni**, è necessario informare in modo chiaro e informativo sull'ambito di applicazione della protezione dellə segnalanti, sulle condizioni per accedere alla protezione prevista dalla legge e garantire esplicitamente che non vi saranno ritorsioni nei loro confronti se le segnalazioni sono fondate. È importante sottolineare che la protezione deve essere garantita anche se una segnalazione risulta non fondata, ma lə segnalante ha ragionevolmente creduto che fosse vera.

C. Per quanto riguarda **la limitazione di responsabilità** (penale, civile e amministrativa), lə segnalante non è punibile qualora la segnalazione riguardi particolari categorie di informazioni. In particolare, non è punibile chi riveli o diffonda informazioni coperte da obbligo di segreto diverso da quello professionale forense e medico, da norme sul diritto d'autore o sulla protezione dei dati personali (cfr. **capitolo 3**), o se al momento della segnalazione aveva ragionevoli motivi per ritenere che tale rivelazione fosse necessaria per effettuare la segnalazione stessa, e questa è avvenuta secondo le modalità previste dalla legge.

D. Per quanto riguarda **la riservatezza** (che garantisce che l'identità di chi segnala non venga rivelata a persone non autorizzate) deve essere spiegato in modo chiaro e semplice in che modo è garantita la riservatezza dellə segnalante, vale a dire: garanzia del principio dell'accesso minimo e dell'integrità dei dati, spiegazione/giustificazione del trattamento dei dati, descrizione del trattamento dei dati durante tutte le fasi del processo, tempo di conservazione e ubicazione delle informazioni, misure di protezione dei dati e dell'identità dellə segnalante, descrizione dei sistemi di anonimizzazione e pseudonimizzazione, descrizione del controllo, del monitoraggio e della segregazione dei *file* delle persone segnalanti da *file* diversi[23], misure per impedire la reidentificazione. Al tempo stesso, occorre garantire l'impossibilità di tracciabilità dell'identità di chi segnala, attraverso l'uso

Cp. 3>

---

[22] *Legge spagnola 2/23 Art. 5.2. Par. h); Legge bulgara Art.13; D.Lgs. italiano 24/2023 Artt. 4, 5, 7, 8, che recepisce la Direttiva (UE) 2019/1937.*

[23] *Le informazioni che identificano o che riguardano direttamente lə segnalante devono essere tenute separate da altri archivi generali (es. file disciplinari, risorse umane, documenti aziendali ordinari): questo isolamento serve a impedire accessi non autorizzati e a preservare l'anonimato o la riservatezza.*

di sistemi *TOR* o protocolli *zero-knowledge proofs* - prove a conoscenza zero). Nel caso in cui il canale o una parte del processo sia esternalizzato, è importante descrivere tutte le misure di sicurezza stabilite dal *provider* e dal *server*. In più: è necessario sviluppare politiche interne per lə segnalanti che dettaglino il regime di riservatezza e i ruoli delle persone responsabili per garantire che l'identità di chi segnala rimanga protetta.

E. È necessario informare sulle caratteristiche fondamentali che garantiscono il completo **anonimato**, qualora lə segnalante scelga questa opzione. Occorre infatti ricordare che la Direttiva contempla la possibilità, pur non incoraggiandola, di **segnalazioni anonime**. **L'anonimato** dovrebbe garantire che una persona che desidera mantenere segreta la propria identità possa essere sicura che ciò avvenga. L'accesso anonimo, e fruibile a tanti, deve rimanere sempre possibile e privo di barriere tecniche, quindi facendo attenzione a forme di accesso che impediscono tale possibilità (si pensi all'autenticazione a due fattori o all'*intranet* aziendale). Secondo alcuni *stakeholder* intervistatə, sono state rilevate alcune caselle di posta elettronica o canali di alcune istituzioni pubbliche[24] che pretendono di garantire l'anonimato, ma in pratica non è così.

1.2.4 Ricevimento, gestione e investigazione degli organi

È poi importante **garantire la trasparenza sull'organo ricevente e l'organo deputato alla gestione** (se separato) della segnalazione, **nonché sull'organo inquirente** e l'**organo di risoluzione**. Tale separazione organizzativa è fondamentale non solo per favorire una maggiore fiducia nel sistema, ma anche per garantire il rispetto del principio di imparzialità e indipendenza in tutti i processi investigativi avviati a seguito delle segnalazioni.

Ricordiamo che:

A. **Organo ricevente**: è l'entità o la persona che riceve la segnalazione, cioè chi riceve /ascolta la segnalazione.
B. **Organo di gestione**: è la persona o il gruppo che si occupa di gestire il processo di segnalazione, ossia organizzare, monitorare e prendere decisioni sul trattamento della segnalazione. In alcuni casi, anche in funzione della dimensione dell'ente e delle normative di recepimento, questo organo potrebbe essere coincidente con l'organo ricevente.
C. **Organo inquirente**: è l'organo che si occupa di investigare sulle segnalazioni (cfr. **capitolo 2**), cioè quello che indaga per capire se ci sono prove di illeciti o violazioni.
D. **Organo di risoluzione**: è l'ente o il gruppo che prende decisioni finali in merito alla segnalazione, stabilendo se le accuse sono fondate o meno e applicando eventuali sanzioni o misure correttive.

Cp. 2 >

È inoltre necessario includere **una spiegazione delle misure** in atto per prevenire potenziali **conflitti di interesse** tra gli organi o i diversi dipartimenti e fornire opzioni alternative se la persona responsabile del sistema o qualsiasi membro degli organi che a diverso titolo intervengono

[24] *Si veda: https://xnet-x.net/es/proliferacion-buzones-anonimos-no-lo-son/*

nella cosa (organi riceventi, di gestione, inquirenti o di risoluzione, nonché seconde istanze o potenziali) sono coinvolti nella segnalazione.

1.2.5. Date e scadenze di riconoscimento, ammissione, indagine e risoluzione

Infine, sempre rimanendo in ambito di trasparenza circa il "contenuto", occorre garantire piena trasparenza sulle tempistiche e le fasi successive all'atto della segnalazione. In concreto:

1) Prima fase

Ai sensi della Direttiva (Art.9.2[25]), **l'avviso di ricevimento** deve essere comunicato al segnalante entro un termine **massimo di sette giorni** di calendario dalla ricezione o dalla registrazione della segnalazione, a meno che ciò non possa mettere a repentaglio la riservatezza.

2) Scadenze di ammissione

Il sito *web* dell'ente deve indicare il termine per le indagini preliminari o per la decisione sull'**ammissibilità della segnalazione**[26]. Tale valutazione implica la raccolta di tutte le informazioni, la documentazione e le prove necessarie. Di conseguenza, l'ente deve informare esplicitamente sui seguenti aspetti:

A. **Termine massimo per lo svolgimento della verifica preliminare di ammissibilità al fine di evitare indebiti ritardi**. Ciò non è previsto dalla Direttiva, né dalla legge italiana, spagnola, o bulgara ma, per esempio, il termine concesso all'Autorità Indipendente spagnola per l'ammissione o il rifiuto di una segnalazione nella Legge 2/2023 è "non superiore a dieci giorni lavorativi dalla data di registrazione della comunicazione". Questo potrebbe essere un buon parametro da considerare a seconda delle caratteristiche e delle capacità dell'ente, ma ciò che si raccomanda è che venga fornito pubblicamente una tempistica chiara al fine di evitare indebiti ritardi.
B. **Termine massimo per la comunicazione allə segnalante dell'ammissione al trattamento o al deposito della segnalazione/ comunicazione**. Anche in questo caso, né la Direttiva europea né la legge italiana, spagnola o bulgara regolano chiaramente questo aspetto. Per esempio, la legge spagnola stabilisce un termine massimo di notifica di "cinque giorni lavorativi", ma non specifica quando questi cinque giorni devono essere conteggiati. A nostro avviso, tale termine dovrebbe decorrere dal momento in cui viene effettuato il test preliminare di ammissibilità (il cui periodo massimo di esecuzione, come indicato in precedenza, sarebbe per esempio di dieci giorni lavorativi

---

[25] *Legge spagnola 2/23 Art. 9.2. Par. c); Legge bulgara, art.5 a) e Legge italiana D.lgs. 24/2023, Art. 7., rispettivamente per i canali interni ed esterni, stabilendo anche un termine di 7 giorni per l'emissione della ricevuta della segnalazione.*

[26] *A questo proposito, si veda Martínez García (2021): "Anonimato, pseudonimia e riservatezza: verso un quadro completo e coerente per la protezione dellə segnalanti".*

dalla data di registrazione[27]), a meno che la segnalazione non sia anonima o lə segnalante abbia rinunciato a ricevere le segnalazioni.

Un altro aspetto importante da considerare è che **né la Direttiva europea né le leggi nazionali specificano termini chiari per la notifica della segnalazione alla persona segnalata** in questa fase procedurale. Ciò solleva dubbi sul fatto che essa abbia il diritto di essere informata della presentazione di una segnalazione che non supera il test preliminare di ammissibilità.

Prendendo il caso della **Spagna**, che fa da esempio generale per gli altri, da un'ampia lettura dell'articolo 18.2. a) 4° della legge spagnola 2/2023, si potrebbe dedurre che tale notifica non è necessaria in quanto stabilisce l'inammissibilità per mancanza di **informazioni nuove o significative** rispetto a una precedente comunicazione "in relazione alla quale sono state concluse le procedure corrispondenti". Tuttavia, questa è una formula proceduralmente ambigua perché:

A. Facendo riferimento a procedure al plurale, potrebbe trattarsi di una comunicazione, che è già stata depositata[28] per non aver superato il test di **ammissibilità**, seguita da una successiva relazione complementare che fornisca nuove prove pertinenti, significative o decisive[29]. Ciò solleva la questione del tempo massimo per la conservazione dei dati personali di un rapporto sul campo[30]. Ad esempio, ai sensi dell'articolo 32.3 della **legge spagnola**, se la segnalazione è inammissibile a causa della causa stabilita nell'articolo 18.2. a) 1° (mancanza di plausibilità) ed è dimostrato che le informazioni fornite o parte di esse non sono veritiere, la legge stabilisce che "deve essere immediatamente cancellata una volta confermata questa circostanza, a meno che tale non veridicità possa costituire un reato, nel qual caso le informazioni saranno conservate per il periodo necessario durante il quale è in corso il procedimento giudiziario" e, in ogni caso, non oltre tre mesi, a meno che lo scopo della conservazione non sia quello di fornire prove del funzionamento del sistema[31], nel qual caso le informazioni devono essere sempre conservate in modo anonimo.
B. Potrebbe anche riferirsi ai casi in cui, dopo che è stato decretato che la persona interessata non viene informata fino alla **fase dell'udienza** a causa di un rischio di **distruzione**, occultamento o alterazione delle prove (articolo 19.2 della legge spagnola 2/23), lə segnalante effettua comunicazioni complementari (ai sensi dell'articolo 18.2.a) 4° della presente legge) e include nuove accuse contro la persona interessata. In tali casi, salvo ancora una volta il rischio di occultamento, distruzione o alterazione delle prove in relazione a queste nuove accuse, la persona interessata deve essere informata secondo la procedura abituale per evitare potenziali indifesi.

---

[27] *Per esempio, se la verifica di ammissibilità è completata l'ottavo giorno lavorativo successivo alla registrazione della comunicazione, l'ente disporrà di ulteriori cinque giorni lavorativi da quel momento per comunicare al segnalante se la sua comunicazione è ammessa, per un totale di tredici giorni lavorativi dalla registrazione della comunicazione.*

[28] *Qualsiasi notifica relativa al deposito di una relazione deve essere sufficientemente motivata.*

[29] *A condizione che queste nuove prove non siano state ottenute in violazione dei diritti o delle libertà fondamentali o illegalmente.*

[30] *A questo proposito, cfr. capitolo 3.*

[31] *Il che può sollevare questioni circa una potenziale riapertura illimitata delle cause presentate durante la fase di valutazione preliminare, sollevando interrogativi legati alla possibile violazione del principio di ne bis in idem.*

3) Scadenze del processo istruttorio

Per quanto riguarda i termini delle indagini, sebbene la Direttiva e le leggi nazionali stabiliscano che le persone siano informate di una eventuale segnalazione nei loro confronti, nonché dei fatti in essa succintamente descritti, non vengono definite tempistiche chiare a riguardo. A tale riguardo, terremo conto del fatto che **l'obbligo di informare le persone di una segnalazione nei loro confronti dovrebbe essere valutato rispetto alla possibilità di ritorsione** e all'identificazione di chi segnala. Tali soggetti devono essere informati quando è necessario difendersi, per esempio in caso di presunte ritorsioni, ma non necessariamente dopo aver ricevuto una segnalazione.

Gli enti devono stabilire tali termini nell'ambito delle loro politiche interne per garantire la tutela dei diritti procedurali della persona segnalata. Ciò include la garanzia del diritto di essere adeguatamente informatə sulle accuse a proprio carico, nonché su eventuali modifiche significative dell'ambito dell'indagine e dei fatti presunti.

Per rimanere all'esempio spagnolo, il Codice di Procedura Penale iberico afferma esplicitamente che "queste informazioni saranno fornite con sufficiente dettaglio per consentire l'effettivo esercizio del diritto di difesa". Ciò implica che la salvaguardia di questo diritto richiede non solo un breve riassunto dei fatti, ma un livello di dettaglio sufficiente a consentire una difesa efficace.

Chi ha scritto questa guida ritiene che, una volta concordata l'ammissione al trattamento di una segnalazione, **si debba applicare alla persona segnalata lo stesso termine massimo di notifica previsto per chi segnala (e in ogni caso mai un termine più lungo)**: cinque giorni lavorativi successivi alla decisione di ammissione della segnalazione al trattamento, per notificarle che è stata ammessa e avviata un'indagine su una segnalazione in cui è coinvolta[32]. Tuttavia, se l'organismo investigativo ritiene che la notifica alla persona segnalata possa comportare un rischio elevato di occultamento, distruzione o alterazione delle prove da parte sua o di terzi, tali informazioni possono esserle fornite durante la fase di audizione[33].

4) Termini di giudizio

Per quanto riguarda i termini di giudizio, deve essere comunicato in modo chiaro e trasparente che il tempo massimo di risposta[34] non deve superare i tre mesi dal ricevimento della comunicazione, salvo casi di particolare complessità che richiedano una proroga fino a un massimo di tre mesi aggiuntivi.

---

[32] Tutto ciò in base al Codice di procedura penale spagnolo (LECrim, Art. 118.5), che stabilisce che: "L'ammissione di una segnalazione o di una denuncia, e qualsiasi azione procedurale che porti all'accusa di un reato contro una o più persone specifiche, deve essere immediatamente portata all'attenzione dei presunti responsabili".

[33] Ai sensi della Legge spagnola 2/2023 Art. 19.2; della Legge bulgara, Art. 16.

[34] Ai sensi della Legge spagnola 2/23, Art. 9.2. Par. d); della Legge bulgara, Art. 16 (per i canali interni) e Art. 23 (per i canali esterni); e Legge italiana Art. 5 (relativi al canale interno) e Art. 8 (relativi al canale esterno).

1.2.6 Regime disciplinare applicabile

Chi ha redatto questa guida ritiene che sia necessario che sia fatta piena e corretta informazione su quali siano le **conseguenze per chi usa in modo scorretto il canale di segnalazione, ad esempio inviando informazioni false o fuorvianti di proposito**, così da evitarne abusi.

Per questo è necessario comunicare che fornire consapevolmente informazioni false, attribuendo a un'altra persona fatti falsi che, se veri, costituirebbero un'infrazione, o affermando falsamente di essere vittima di un illecito può costituire reato o illecito amministrativo. In **Italia**, la legge prevede sanzioni amministrative nei confronti di unə segnalante che presenta consapevolmente false segnalazioni. La persona o l'ente, a cui viene attribuita falsamente la commissione di una violazione, deve segnalare ciò alle autorità competenti.

1.2.7. Dati di contatto utili dei canali esterni e dei servizi civici di supporto

Occorre dare informazione anche circa i recapiti dei canali ufficiali esterni[35] includono: gli indirizzi e-mail e postali e i numeri di telefono associati a tali canali; i recapiti dell'autorità indipendente e delle[36] altre autorità competenti per la ricezione di tali segnalazioni.

Altra informazione utilissima da offrire a chi intende segnalare è la possibilità di ricevere ascolto e supporto tramite quelli che la Direttiva chiama "**centri di informazione**".

A riguardo, l'articolo 20 della Direttiva riconosce infatti il ruolo di tali centri (cfr. capitolo 2) come servizi di supporto che (anche) la **società civile** può organizzare e mettere a disposizione per aiutare i potenziali segnalanti ad affrontare dilemmi etici e dubbi sul funzionamento del sistema. La legge stabilisce che questo ruolo possa parimenti essere svolto da **istituzioni dedicate**.

Cp. 2 >

Accedere, in fase di dilemma etico, a questa forma di sostegno può fare la differenza per chi intende segnalare, al fine di ricevere ascolto, supporto, orientamento. Pertanto, è bene che tanto dalle pagine predisposte per i canali interni quanto per quelle dei canali esterni si possa accedere a una risorsa che contenga i contatti diretti con tali centri di ascolto, informazione e supporto.

In **Italia**, dal 2024 **ANAC ha predisposto una pagina dedicata che riporta i nomi delle associazioni che offrono questo tipo di servizi**[37]. Nella presente guida, incoraggiamo a facilitare quanto più possibile la conoscenza di tali centri.

---

[35] *Legge spagnola 2/23 titolo III; Legge bulgara Art. 21 e Legge italiana Art. 9 (per il canale esterno, gestito dall'ANAC)*

[36] *In Spagna l'Autorità Indipendente per la Protezione dellə Segnalanti (A.A.I.), in Italia l'Autorità Nazionale Anticorruzione, in Bulgaria la Commissione per la Protezione dei Dati Personali.*

[37] *Si veda: https://www.anticorruzione.it/-/whistleblowing#p10*

FOCUS GOVERNO APERTO

Gli *stakeholder* di tutti i settori suggeriscono che **un approccio collaborativo** che coinvolga le organizzazioni della società civile (OSC) e le autorità pubbliche **può migliorare le pagine informative e i sistemi di segnalazione, garantendone la chiarezza e una prospettiva orientata allə segnalanti**. Ciò significa rendere le procedure di segnalazione accessibili e di facile comprensione.

In linea con ciò, le organizzazioni della società civile suggeriscono strategie semplici ma efficaci per migliorare l'usabilità dei contenuti e aumentare la fiducia nei canali di segnalazione:

A. Usare un linguaggio semplice e facile da capire, evitando il gergo tecnico o legale.
B. Fornire esempi pratici quando possibile.
C. Ripetere le istruzioni chiave per la segnalazione durante tutto il processo di segnalazione, anche nella pagina delle informazioni e all'interno del canale stesso di segnalazione.
D. Nella piattaforma o nel modulo di segnalazione, richiedere prima l'oggetto della segnalazione e solo alla fine il nome della persona segnalante.

Per migliorare i sistemi di segnalazione e le pagine informative, **consultazioni pubbliche aperte a tutte le parti interessate possono contribuire a perfezionare i contenuti e l'usabilità** e quindi incoraggiare la segnalazione. L'autorità competente dovrebbe condurre tali consultazioni, dando l'esempio ad altri soggetti obbligati affinché riproducano i risultati ottenuti o promuovano le proprie consultazioni pubbliche.

Le migliori pratiche di governo aperto includono **l'inclusione di informazioni chiare sui siti *web* delle autorità pubbliche in merito ai servizi di consulenza e supporto allə segnalanti** gestiti dalle istituzioni (per esempio, l'ufficio del difensore civico) e dalle organizzazioni della società civile. Questa disposizione non è esplicitamente disciplinata dalla Direttiva (UE) 2019/1937. Tuttavia, siccome stabilisce solo norme minime, gli Stati membri dell'UE che desiderano andare oltre i suoi requisiti e includere tale disposizione nelle loro leggi o regolamenti nazionali sono fortemente incoraggiati a farlo.

Per esempio, **il 5° Piano d'Azione Nazionale (5NAP)** per il governo aperto (2021-2023) dell'Italia[38], si è incentrato sul **rafforzamento della collaborazione tra gli attori istituzionali e della società civile nel lavoro di sensibilizzazione e di sostegno ai soggetti segnalanti.**

I principali risultati includono:

A. **Promuovere la visibilità e l'accessibilità ai servizi di supporto delle OSC**: l'Autorità Nazionale Anticorruzione (ANAC) ha guidato una *task force* che coinvolge la società civile e le pubbliche amministrazioni per individuare pratiche volte a migliorare gli *standard* di protezione dei soggetti segnalanti e la qualità delle segnalazioni. Attraverso una serie di dialoghi congiunti con l'ANAC, i contributi delle organizzazioni della società civile sono stati integrati nel processo di recepimento legislativo della Direttiva europea, influenzando l'inclusione di un elenco pubblico delle organizzazioni della società civile che supportano lə segnalanti sul sito *web* dell'ANAC. In questo modo, lə potenziali segnalanti che accedono al sito dell'ANAC per conoscere le procedure di segnalazione e le relative tutele vengono anche immediatamente a conoscenza dei servizi di supporto a loro dedicati. Ciò ha dimostrato di avere un effetto a catena positivo, in quanto altre pubbliche amministrazioni italiane hanno a loro volta adottato la buona pratica di aumentare la visibilità dei servizi della società civile fornendo un *link* diretto al loro sito *web*.
B. **Rafforzare le competenze dellə dipendenti pubblicə attraverso una Comunità di Pratica (CdP):** sotto la guida della Scuola Nazionale di Amministrazione (SNA), è stata creata la Comunità di Pratica dellə funzionarə formalmente incaricatə della prevenzione della corruzione nelle pubbliche amministrazioni italiane (RPCT): uno spazio collaborativo in cui lə RPCT possono scambiare conoscenze, condividere le migliori pratiche e migliorare le loro capacità di prevenire la corruzione all'interno delle rispettive organizzazioni. Al fine di rafforzare le capacità dellə dipendenti pubblicə di

[38] *Si veda:* https://www.opengovpartnership.org/members/italy/

gestire le segnalazioni di *whistleblowing* e aumentare la loro più ampia consapevolezza in merito al tema, la CdP ha organizzato quattro appuntamenti di formazione sul *whistleblowing* e ha superato gli obiettivi di partecipazione. È stato pubblicato un manuale completo per guidare lə professionistə[39] e sono state sviluppate tre buone pratiche in materia di *whistleblowing*[40]. I materiali di formazione e orientamento sono fondamentali per diffondere l'informazione sui sistemi di segnalazione internamente ed esternamente alle pubbliche amministrazioni.

Per aumentare il senso di responsabilità collettiva dei meccanismi di *whistleblowing*, tutti i soggetti obbligati possono promuovere la formazione dellə proprə dirigenti e dipendenti. Nell'esperienza delle organizzazioni della società civile, la **formazione rivolta allə dipendenti di tutti i settori dovrebbe** allontanarsi da un approccio incentrato sul diritto e **adottare invece un approccio basato sul dilemma etico**. Attraverso questa metodologia, che è esperienziale più che teorica, lə partecipanti riflettono su casi prototipici di cattiva condotta, lavorando sia individualmente che in gruppo per identificare possibili soluzioni, tra cui le segnalazioni di *whistleblowing*, aiutandolə a simulare una segnalazione. I moduli di formazione possono essere organizzati in forme congiunte dalle istituzioni e da altre parti interessate, come nell'esempio del progetto "*Open the Whistle*".

Ulteriori iniziative coerenti con i principi di trasparenza e collaborazione del governo aperto possono consistere nella promozione di **campagne di comunicazione congiunte** tra diversi *stakeholder*, seguendo l'esempio di "*Open the Whistle*", o nell'utilizzo dei media radiotelevisivi nazionali per progetti di comunicazione con valore sociale. Le piattaforme popolari, come quelle legate a eventi sportivi o culturali, possono fornire opportunità di comunicazione dirette a un pubblico molto ampio.

1.3 TRASPARENZA DEI SISTEMI E DEI CANALI INFORMATIVI: REQUISITI FORMALI

Prima di questo lungo elenco sugli aspetti di "contenuto", abbiamo già detto come occorra il rispetto anche di **requisiti di carattere formale**. Significa che **le informazioni devono essere chiare, corrette, complete e facilmente accessibili**.

L'accesso deve essere universale, il che significa che tuttə lə potenziali destinatarə devono avere pari opportunità di accedere alle informazioni. Ciò richiede l'adozione di metodi inclusivi per tutti gli individui. Secondo l'Organizzazione Mondiale della Sanità (OMS), più di un miliardo di persone in tutto il mondo hanno una qualche forma di disabilità e, di queste, quasi 200 milioni sperimentano notevoli difficoltà nel loro funzionamento quotidiano[41]. I tipi più comuni di disabilità sono solitamente visive, uditive, motorie e cognitive.

[39] *Si veda: https://sna.gov.it/wp-content/uploads/2024/09/WHISTLEBLOWING-cultura-integrita.pdf*

[40] *La prima sottolinea la necessità di non dimenticare come lə segnalanti siano persone, non solo un'istituto giuridico; la seconda buona pratica si concentra sullo sviluppo di politiche che trattino il whistleblowing come un dovere piuttosto che un'attività rischiosa, al fine di eliminare lo stigma sociale e normalizzare l'atto di denunciare illeciti; il terzo sottolinea il ruolo delle organizzazioni della società civile (OSC), fornendo un link diretto al loro sito web sulla piattaforma di whistleblowing delle Pubbliche Amministrazioni. Si veda: https://sna.gov.it/home/attivita/comunita-di-pratica/comunita-di-pratica-per-rpct/buone-pratiche/whistleblowing-buone-pratiche/*

[41] *Si veda: https://www.paho.org/es/noticias/5-12-2011-mil-millones-personas-viven-con-discapacidades#:~:text=M%C3%A1s%20de%20mil%20millones%20de,pues%20su%20prevalencia%20est%C3%A1%20aumentando*

In Italia[42], il D.Lgs. 76/2020, recante modifica della Legge 4/2004 con l'introduzione del comma 1 bis all'Art. 3, ha esteso l'applicazione degli obblighi di accessibilità ai soggetti privati, oltre che ai siti *web* del settore pubblico, che già dovevano essere accessibili. Per estensione, ciò vale anche per i canali di *whistleblowing*.

Allo stesso modo, in **Spagna** devono essere presi in considerazione sia il Regio Decreto 1112/2018 del 7 settembre, sull'accessibilità dei siti *web* e delle applicazioni per dispositivi mobili del settore pubblico, sia le Linee guida per l'accessibilità dei contenuti *Web* (WCAG) sviluppate dal *World Wide Web Consortium* (W3C).

In coerenza con queste linee guida, **è importante evitare alcune pratiche sui siti *web*,** come posizionare elementi cliccabili molto vicini tra loro e utilizzare icone molto piccole o *link* di testo con dimensioni dei caratteri eccessivamente ridotte. Si consiglia inoltre di prestare attenzione ai corretti contrasti tra le combinazioni di colori dello sfondo e del testo. In questo senso, le WCAG definiscono nel Criterio 1.4.3 i parametri che devono essere seguiti per ottenere il contrasto cromatico[43].

Inoltre, **in queste pagine sconsigliamo fortemente l'utilizzo dell'*intranet*** come forma di accesso al canale di segnalazione, poiché limita l'accessibilità di un grande numero di persone che hanno diritto di utilizzare il canale di segnalazione interna. Inoltre, può compromettere la percezione di riservatezza e indipendenza necessaria a generare fiducia nel sistema.

Infine, si raccomanda di includere, per facilitare la comprensione e l'accessibilità, **una sezione di domande frequenti (FAQ) o video esplicativi** sul funzionamento di base del canale *whistleblowing*. Inoltre, quando i file multimediali o audiovisivi sono messi a disposizione dellə utenti, devono includere sottotitoli, trascrizioni audio e descrizioni video per garantire l'accesso alle persone con disabilità uditive.

1.4 TRASPARENZA DEI SISTEMI E DEI CANALI INFORMATIVI: RELAZIONI ANNUALI E STATISTICHE

Oltre ai finora citati aspetti di "contenuto" e "forma", che sono obbligatori, esistono altre informazioni la cui trasparenza e la cui pubblicazione concorrono a creare fiducia nel sistema, oltre che fungere come esercizio di buona *governance*. Su tutte (e per come si vedrà più approfonditamente nel capitolo 5), **la pubblicazione periodica dei dati sulle prestazioni del sistema sulle relazioni annuali**.

Cp. 5

Come buona prassi, raccomandiamo quindi di **fornire informazioni statistiche** al pubblico e alle parti interessate, almeno una volta all'anno, **sui seguenti settori:**

---

[42] *Per ulteriori informazioni, si veda: https://www.agid.gov.it/it/ambiti-intervento/accessibilita-usabilita*

[43] *Per esempio, per il livello AA, è richiesto un rapporto di contrasto di 4,5:1 tra lo sfondo e il testo.*

A. Numero e tipologia di comunicazioni ricevute.
B. Numero di comunicazioni accettate per l'elaborazione.
C. Numero di comunicazioni respinte dopo l'esecuzione della verifica di ammissibilità.
D. Numero di comunicazioni analizzate che terminano con una risoluzione.
E. Numero di comunicazioni indagate che hanno portato all'adozione di misure volte a ridurre o evitare i fattori di rischio rilevati.
F. Numero di comunicazioni indagate che sono state infine archiviate.
G. Numero di sanzioni irrogate o procedimenti disciplinari avviati.
H. Numero di volte in cui l'ente ha deferito casi alla Procura della Repubblica, alla Procura europea, alle autorità indipendenti o agli organi giurisdizionali.
I. Numero di sessioni di formazione svolte per dipendenti e manager sul canale di segnalazione.
J. Numero di segnalazioni riservate e numero di segnalazioni anonime.
K. Numero di casi in cui l'ente ha incaricato una società esterna di assumere servizi investigativi o esperti di conformità forense.
L. Numero e tipologia delle misure di sostegno[44] o di altre misure fornite volontariamente.
M. Nel caso di un'organizzazione con presenza internazionale: numero di comunicazioni ricevute per area geografica.
N. Numero e tipologia di miglioramenti apportati al sistema informativo e al canale.
O. Risultati generali riguardanti il livello di soddisfazione, consapevolezza e comprensione del sistema tra lə suə utenti.

Ovviamente **tali relazioni o conti annuali non devono includere dati personali**, in particolare dati che consentano l'identificazione o la reidentificazione di segnalanti, persone interessate, testimoni o terzi coinvolti in qualsiasi processo, anche se tali dati sono già stati pubblicati a seguito di una sentenza definitiva.

1.5 AZIONI DI SENSIBILIZZAZIONE INTERNA ED ESTERNA

Un'altra prassi che possiamo intendere in termini di trasparenza, quindi coerente con questo capitolo, sono le **strategie di comunicazione**. Se ben progettate, esse garantiscono accessibilità e fiducia tra lə segnalanti. Tuttavia, persistono diverse sfide, come la mancanza di conoscenza dei canali di segnalazione, la percezione negativa dellə segnalanti in alcune culture, il timore di ritorsioni e l'assenza di efficaci campagne di sensibilizzazione.

1.5.1 Comunicazione interna: sfide e best practice

Mancanza di chiarezza e formazione insufficiente

[44] *Descritto nella Legge spagnola 2/2 Art. 37; nella legge bulgara Art.13; nel D.lgs. italiano Art.18.*

Le interviste condotte nei tre Paesi hanno rivelato che moltə dipendenti non sono a conoscenza di come segnalare illeciti e i canali di segnalazione interni non sono ben documentati. Per affrontare questo problema, è **consigliabile organizzare formazione periodiche,** integrare la **sensibilizzazione sul *whistleblowing*** nei programmi di inserimento dellə dipendenti e rafforzare le **campagne di comunicazione interne** che evidenziano l'importanza della segnalazione. Come buona prassi, alcune aziende hanno implementato codici QR con istruzioni chiare per facilitare l'accesso al canale di segnalazione.

Diffidenza, percezione negativa e necessità di un'azione comunitaria

Ancora oggi, nonostante un cambiamento culturale lentamente in atto, il *whistleblowing* è ancora percepito come una forma di tradimento, specie in alcuni contesti. Le interviste hanno indicato che la paura è l'ostacolo principale, rendendo fondamentale un cambiamento nella narrazione. Per ovviare a questo, le strategie di comunicazione possono **enfatizzare il *whistleblowing* come una responsabilità etica**, supportata da testimonianze di dipendenti o *manager* che ne sottolineino l'importanza.

Ancor più, ed è la direzione che questa guida sostiene con più forza, è necessario, attraverso campagne comunicative innovative e "nazionalpopolari", **valorizzare la dimensione collettiva del *whistleblowing***: il suo impatto sulla società, la costruzione di una comunità solidale attorno a chi segnala, la necessità di rompere l'isolamento. Ciò contribuirebbe effettivamente a generare una nuova narrativa attorno all'istituto.

Integrazione con le politiche etiche e di compliance

Le interviste hanno anche indicato che molte aziende non hanno un reale impegno nella gestione delle segnalazioni. Per rafforzare questi meccanismi, **i sistemi di *whistleblowing* devono essere integrati negli *audit* interni e nei sistemi di controllo dei rischi**, garantendone l'integrazione nella *governance* aziendale. Ove ciò avviene, andrebbe pubblicamente comunicato.

1.5.2 Comunicazione esterna e coinvolgimento degli stakeholder

Mancanza di trasparenza e scarsa capacità nella comunicazione pubblica

Per come registrato le interviste realizzate per questa guida, molte organizzazioni non riescono a comunicare in modo efficace i loro sistemi di *whistleblowing*. Una misura per cambiare la narrativa potrebbe essere la **pubblicazione di statistiche e storie di successo per creare fiducia.**

Pertanto in questa guida suggeriamo, a chi si appresta a organizzare una campagna sul tema, di **resistere alla tentazione di raccontare soltanto le storie di chi è diventatə notə dopo aver segnalato**. Di per sé, unə segnalante di cui conosciamo l'identità rappresenta un ossimoro: il nome non dovrebbe mai emergere pubblicamente, a meno che non sia la stessa persona segnalante a volerlo. Occorre quindi prestare attenzione agli **effetti *boomerang*** che possono derivare da azioni comunicative improvvisate, mal gestite o poco consapevoli delle possibili ricadute.

Non si tratta di negare spazio o voce a chi ha scelto di esporsi, soprattutto se ha subito ritorsioni: chi ha segnalato conosce infatti spesso a fondo le falle del sistema e può dare un contributo fondamentale nei percorsi di *advocacy*. Non è però detto che siano le persone più adatte a rappresentare l'istituto in campagne pubbliche. A volte, **raccontare il *whistleblowing* non coincide con il raccontare la storia di chi lo ha vissuto**.

Ruolo della società civile e dei media

Secondo alcune intervistate in **Italia** e **Spagna**, specie sul fronte dell'organizzazione di azioni di comunicazione **la società civile può svolgere un ruolo fondamentale per migliorare la trasparenza e promuovere l'istituto,** poiché a volte lo stigma che circonda il *whistleblowing* continua a colpire lə segnalanti e a limitarne la partecipazione. In coerenza con la filosofia che guida la presente guida (scritta assieme da autorità e organizzazioni del terzo settore) invitiamo a stabilire canali di dialogo tra istituzioni, *media* e organizzazioni del terzo settore, al fine di rafforzare l'*accountability* e ampliare la portata dei meccanismi di segnalazione.

1.6 RACCOMANDAZIONI

1. MAGGIORE CHIAREZZA

Una maggiore chiarezza sui canali e sui processi di *reporting* interno è fondamentale, sia sul lato formale che di contenuto.

2. CAMBIAMENTO DI PERCEZIONE

Cambiare la percezione del *whistleblowing* come strumento etico è strategico per favorirne l'uso.

3. DIMENSIONE COLLETTIVA

Valorizzare la dimensione collettiva del *whistleblowing* può fare la differenza.

4. GARANTIRE LA TRASPARENZA

Garantire una trasparenza completa e significativa[45] è essenziale per costruire maggiore fiducia[46].

5. ACCESSO AL SUPPORTO

Far conoscere i centri (civici e istituzionali) di supporto aiuta chi si trova in dilemma etico a non sentirsi solə e a fare una buona segnalazione.

6. TUTELA E INCLUSIVITÀ

Generare strategie inclusive, con una prospettiva di genere e protezione per lə segnalanti più esposte a rischi non è solo opzionali ma necessario.

7. FORMAZIONE DIFFUSA

Maggiore formazione allə lavoratorə, cittadinə e anche allə responsabili della gestione dei sistemi interni di segnalazione contribuisce alla conoscenza dell'istituto.

8. COMUNICAZIONE ATTENTA

Fare attenzione a come si comunica il *whistleblowing* evita effetti *boomerang*.

9. COINVOLGIMENTO DELLA SOCIETÀ CIVILE

Includere la società civile in campagne di comunicazione aiuta a raggiungere innovatività ed efficacia.

CONCLUSIONI: CULTURA DELLA TRASPARENZA

In sintesi: rafforzare la trasparenza e la comunicazione contribuirà a creare una cultura del *whistleblowing* efficace, accessibile e affidabile, promuovendo l'integrità all'interno delle organizzazioni pubbliche, private e del terzo settore.

---

[45] *È molto importante spiegare sui siti web i passaggi per spiegare allə segnalanti cosa devono fare e quali sono le procedure e i loro diritti e obblighi.*

[46] *Secondo uno dei nostri intervistati, sarebbe importante per le Amministrazioni includere anche strumenti, risorse e dati di contatto sulle organizzazioni della società civile che supportano llə segnalanti.*

Correttezza delle indagini e della gestione nell'ambito dei sistemi interni di segnalazione

Capitolo 2

Open the whistle

CORRETTEZZA DELLE INDAGINI E DELLA GESTIONE NELL'AMBITO DEI SISTEMI INTERNI DI SEGNALAZIONE

CAPITOLO 2

2.1 ELEMENTI CHIAVE PER UNA CORRETTA INDAGINE

Uno degli aspetti cruciali dell'istituto del *whistleblowing* riguarda **le modalità con cui si conduce un'indagine interna a seguito di una segnalazione**. In queste pagine proveremo ad approfondire le questioni più rilevanti legate a tale snodo delicato.

Partiamo dall'inizio: quando una segnalazione interna è fatta in coerenza con la normativa (sia quella della Direttiva che le leggi specifiche di ciascun Paese), deve essere avviata un'**indagine interna** che rispetti tutte le garanzie giuridiche e venga gestita con la massima attenzione e rigore. L'indagine interna è un processo formale e sistematico che ha l'obiettivo di esaminare la segnalazione, verificare i fatti e, se necessario, prendere le misure appropriate per risolvere la situazione. Le forme di protezione (che vedremo nel **capitolo 4**) sono poi la chiave per rompere il silenzio e incoraggiare chi ha informazioni rilevanti a farsi avanti senza paura.

Cp. 4>

L'articolo 7 della Direttiva europea (commi 1 e 2) stabilisce espressamente il principio secondo cui **le persone segnalanti sono incoraggiate (letteralmente) a effettuare una prima segnalazione tramite canali interni o, solo a certe condizioni, direttamente tramite canali esterni.** La segnalazione esterna è prevista, in particolare, nei casi in cui la violazione non possa essere affrontata efficacemente a livello interno o quando la persona segnalante ritiene che vi sia rischio di ritorsioni (cfr. Art. 7, comma 2).

Qui già si apre una prima questione: alcuni Stati membri **impongono erroneamente l'obbligo di effettuare prima una segnalazione interna o consentono la comunicazione esterna diretta solo in circostanze specifiche**.

In **Italia**, la segnalazione interna è indicata come **il primo passo da compiere** in aderenza alla Direttiva, lasciando aperta la possibilità di segnalare direttamente al canale esterno (ANAC) in presenza di quelle condizioni espressamente previste dalla Direttiva.
Al netto della Direttiva stessa, secondo alcune persone intervistate la segnalazione interna non dovrebbe mai essere un prerequisito obbligatorio

per ricorrere ai canali esterni, ma che rimanesse preferibile in quanto può offrire una prima opportunità per risolvere la questione senza dover immediatamente ricorrere a canali esterni, agendo tempestivamente e riducendo le minacce al pubblico interesse.

Chi ha redatto questa guida è concorde con quanto emerso dalla seconda riunione del gruppo di espertə della Commissione Europea sulla Direttiva[47] , la quale ha rilevato che quando lə segnalanti effettuano una segnalazione diretta tramite canali esterni, le organizzazioni non sono in grado di porre tempestivamente rimedio alla situazione o all'irregolarità. Al tempo stesso, nelle organizzazioni della società civile **rimane la preoccupazione che le precondizioni richieste al fine di accedere al canale esterno** (lo si ripete, espressamente previste dalla Direttiva) **possano divenire qualcosa da dimostrare da parte dellə segnalante**, scoraggiando di fatto la segnalazione stessa.
A ogni modo, il rapporto tra i canali di segnalazione resta un tema dibattuto sia nei singoli Stati membri che nel più ampio contesto europeo. La Direttiva ha lasciato agli Stati una certa discrezionalità nel definire modalità e canali di segnalazione e le scelte adottate non sono state uniformi.

Di conseguenza, come già detto nel capitolo precedente, le organizzazioni devono creare canali interni chiari, facilmente accessibili ed efficaci e promuovere una **cultura aziendale e organizzativa che incoraggi attivamente la segnalazione interna** delle violazioni. Le indagini interne derivanti da segnalazioni o informazioni ricevute tramite canali interni, sia all'interno di un'organizzazione pubblica che privata, sono condotte nell'interesse pubblico.

Prima di poter riflettere su come condurre un'indagine, è utile riepilogare brevemente i requisiti fondamentali che le procedure di segnalazione interna e le relative azioni successive devono rispettare, sia per raggiungere gli obiettivi previsti, sia per essere conformi alla Direttiva e alla normativa nazionale. I principali requisiti sono i seguenti:

A. I canali interni devono permettere alle persone interessate dalla Direttiva di segnalare le violazioni previste dalla Direttiva e dalle leggi nazionali di recepimento.
B. I canali devono essere progettati, creati e gestiti in modo sicuro per garantire la riservatezza dell'identità della persona segnalante e di qualsiasi terza parte menzionata nella segnalazione, proteggendo al contempo i dati personali da accessi non autorizzati.
C. Un avviso di ricevimento deve essere rilasciato alla persona segnalante entro sette giorni dal ricevimento della segnalazione.
D. La comunicazione con lə segnalante può essere mantenuta durante l'elaborazione della segnalazione e, se necessario, possono essere richieste ulteriori informazioni.
E. I canali devono consentire un attento seguito e un'elaborazione efficace

[47] *Il gruppo di espertə della Commissione Europea è un gruppo consultivo composto da espertə che rappresentano gli Stati membri dell'Unione europea con responsabilità per il recepimento della Direttiva (UE) 2019/1937. La sua missione fondamentale è quella di formulare raccomandazioni per gli Stati membri per il recepimento della Direttiva.*

delle segnalazioni inviate, comprese quelle anonime, se previste.

F. Devono essere fornite informazioni chiare e accessibili sui canali esterni gestiti dalle autorità nazionali competenti e, nel caso, dalle istituzioni o dagli organi dell'UE.

FOCUS GENERE

L'attuazione di canali sensibili alla dimensione di genere e di politiche mirate migliorerebbe l'efficacia dei processi di sostegno, in particolare per le donne e altri gruppi vulnerabili.

Le raccomandazioni specifiche per garantire meccanismi di segnalazione sensibili alla dimensione di genere possono includere:

A. **Garantire la partecipazione delle donne** e delle diverse identità di genere nella progettazione dei meccanismi e delle politiche di *whistleblowing*.

B. **Stabilire protocolli sensibili al genere** per ogni canale di segnalazione interna.

C. **Coordinare meglio i diversi strumenti già esistenti** come il codice di condotta, le misure per la prevenzione della corruzione e i meccanismi di segnalazione della violenza di genere.

D. **Garantire sistemi di segnalazione e indagine sensibili alle questioni di genere, affiancati da servizi di supporto completi**. Devono essere previste linee guida chiare per la gestione dei casi legati al genere, con personale qualificato in grado di affrontare le segnalazioni con la necessaria sensibilità. È inoltre importante informare lə segnalanti sull'esistenza di servizi di supporto esterni, come assistenza legale, supporto psicologico e organizzazioni di supporto alle vittime.

E. **Sviluppare un canale dedicato** per le richieste relative a comportamenti scorretti e discriminatori basati sul genere. **Fornire una sezione Domande frequenti (FAQ) o linee guida chiare** per la segnalazione di questioni legate al genere.

F. **Condurre corsi di sensibilizzazione sulle questioni di genere** all'interno delle organizzazioni che ospitano canali di segnalazione, così da affrontare gli stereotipi e i pregiudizi di genere per garantire un sistema di *whistleblowing* inclusivo ed efficace.

2.2 CRITICITA' NELLE INDAGINI INTERNE

Stante il predetto, le indagini interne hanno lo scopo di accertare la veridicità o la plausibilità dei fatti segnalati e di individuare eventuali responsabili della violazione o dell'irregolarità. Altro aspetto introduttivo cruciale, per la legittimità delle indagini quanto per il rispetto della Direttiva europea e delle normative nazionali, è che **i metodi utilizzati per la raccolta delle prove garantiscano sempre il rispetto dei diritti fondamentali** (cfr. capitolo 1).

Cp. 1 >

Quali sono le **criticità che possono sorgere durante l'indagine interna**?

A. **Mantenere la riservatezza dei dati personali** può essere complesso e **richiede l'attuazione di specifiche misure tecniche, organizzative e di sicurezza** (come l'accesso limitato e gerarchico, la doppia autenticazione, l'anonimizzazione interna, ecc.) esplicitamente progettate per questo scopo. Durante le indagini interne, l'identità dellə segnalante potrebbe essere scoperta o dedotta inavvertitamente, poiché alcune caratteristiche personali o professionali (come il genere, il ruolo lavorativo o il coinvolgimento in uno specifico progetto) possono rendere la persona identificabile. Inoltre, la richiesta di informazioni ad altri dipartimenti o lo svolgimento di interviste personali possono inevitabilmente ampliare la cerchia di persone a conoscenza dell'indagine e potenzialmente dell'identità del soggetto segnalante.

B. Garantire **la riservatezza dell'identità dei segnalanti**, in particolare **quando i canali di segnalazione interni sono esternalizzati a terzi**, può rappresentare una sfida in più. Tale esternalizzazione deve essere in linea con quanto indicato nel Considerando 54 della Direttiva, che specifica che le terze parti possono includere fornitori di piattaforme di segnalazione esterne, consulenti esterni, revisori, rappresentanti sindacali o rappresentanti dellə lavoratorə. L'esternalizzazione dei servizi aumenta intrinsecamente il numero di persone con accesso alle informazioni sensibili. Pertanto, le garanzie esplicite di indipendenza e riservatezza devono essere chiaramente delineate nell'accordo contrattuale tra l'organizzazione e il terzo esterno. Ai sensi della Direttiva Art. 8, Par. 5, in caso di violazione, sia il fornitore dei servizi che l'ente appaltante condividono la responsabilità. Lə espertə ritengono che la responsabilità solidale sia il modo più efficace per proteggere i diritti della persona segnalante, consentendo a quest'ultima di avviare azioni legali contro l'ente, il fornitore esterno o entrambi.

C. **Il trattamento dell'identità dellə segnalante configura, a tutti gli effetti, un trattamento di dati personali** (cfr. capitolo 3), soggetto alle disposizioni del Regolamento (UE) 2016/679 (GDPR). Per questo, diversə espertə raccomandano che la violazione della riservatezza in questi casi sia sanzionata più severamente rispetto alle violazioni ordinarie della normativa sulla protezione dei dati personali. La ratio è evidente: rivelare l'identità di chi segnala espone quest'ultimə a ritorsioni e mina la fiducia nell'intero sistema di segnalazione.
In alcuni Paesi, le sanzioni previste per la violazione della riservatezza non risultano coerenti, a causa della **mancanza di un adeguato coordinamento con la normativa sulla protezione dei dati**. Questa carenza è preoccupante sia perché segnala una scarsa armonizzazione tra le legislazioni nazionali, sia perché compromette uno dei capisaldi della Direttiva europea: la protezione effettiva dellə segnalante.

Cp. 3 >

D. Infine, durante le indagini interne entrano in gioco anche interessi

organizzativi. In alcuni contesti, le indagini su violazioni o irregolarità sono viste come **forme di collaborazione tra pubblico e privato**. Tuttavia, le interviste condotte in Italia hanno evidenziato un nodo critico: possono emergere conflitti d'interesse, soprattutto quando la segnalazione coinvolge direttamente soggetti apicali o decisioni dell'organizzazione stessa.

FOCUS GOVERNO APERTO

Un'indagine e una gestione efficaci nei sistemi di segnalazione interna richiedono **trasparenza e linee guida ben definite** per garantire coerenza ed equità nei diversi settori, tra cui il settore pubblico, il settore privato e il terzo settore.

Tali linee guida possono essere sviluppate attraverso un approccio di co-progettazione, coinvolgendo le autorità pubbliche responsabili del *whistleblowing* e gli *stakeholder* interessati. Questo processo collaborativo può avvenire attraverso **dialoghi o consultazioni pubbliche**, come dimostrato dall'Autorità Nazionale Anticorruzione (ANAC) in Italia.

Nel 2024, in Italia **l'ANAC ha avviato una consultazione pubblica online**[48] per raccogliere *feedback* sulla sua bozza di linee guida per il *whistleblowing*. L'obiettivo era quello di promuovere un'applicazione uniforme ed efficace della normativa su questa materia, riducendo al contempo le incertezze interpretative per i soggetti che gestiscono le segnalazioni interne sia in organizzazioni pubbliche che private. Il modello ANAC fornisce un quadro utile che altri Paesi potrebbero replicare per migliorare il coinvolgimento degli *stakeholder* nello sviluppo delle linee guida per il *whistleblowing*:

A. Un periodo di consultazione online aperta della durata di almeno un mese per consentire un ampio margine di *feedback*.
B. Una piattaforma di facile utilizzo per l'invio di contributi (per esempio, questionari online).
C. Diffusione capillare dell'iniziativa in diversi forum pertinenti per garantire visibilità e incoraggiare la partecipazione.
D. Inviti mirati ai principali *stakeholder* coinvolti attivamente nei processi di *whistleblowing*.

Gli operatori raccomandano di designare un **punto di contatto (*Point of Contact*) dedicato all'interno dell'autorità pubblica responsabile del *whistleblowing***. Questa persona o ufficio fungerebbe da risorsa di riferimento per i responsabili dei canali di segnalazione interna, fornendo indicazioni e risolvendo le criticità nella gestione e nell'indagine delle segnalazioni. Inoltre, le preoccupazioni relative alle indagini potrebbero essere affrontate attraverso riunioni tra pari tra i gestori dei canali di segnalazione interni e l'autorità pubblica. Per promuovere la collaborazione e il miglioramento continuo, la creazione di un **gruppo di lavoro o di una comunità di pratica** sul *whistleblowing* potrebbe essere incorporata nell'*Open Government Partnership*, sia come parte dei regolari Piani d'Azione Nazionali che come impegno *Open Gov Challenge*.

Un ulteriore aspetto fondamentale per facilitare le indagine interne è garantire l'alta qualità delle segnalazioni di *whistleblowing*. Un modo efficace per progettare un solido sistema di segnalazione interna, che sia il più accurato possibile e allineato con i rischi effettivi affrontati dall'organizzazione (pubblica o privata), è condurre una **valutazione partecipativa dei rischi di potenziali comportamenti scorretti che potrebbero emergere attraverso il *whistleblowing***.

[48] *Si veda:* https://www.anticorruzione.it/en/-/news.07.11.24.lg.whistleblowing

Idealmente, questo processo dovrebbe **coinvolgere più dipartimenti, aree e settori all'interno dell'organizzazione**. Tuttavia, in particolare nel caso delle istituzioni pubbliche, può anche essere realizzato utilizzando i principi del governo aperto, coinvolgendo la società civile e altri attori esterni. Gli *input* esterni possono fornire una prospettiva più ampia e una comprensione più profonda dei fattori ambientali e contestuali, aiutando l'organizzazione a identificare i rischi che altrimenti potrebbero essere trascurati o sottovalutati. Il risultato di questo processo è un sistema di segnalazione che include scenari di casi ben definiti, adattati a una comprensione più profonda dei rischi dell'organizzazione. Questo non solo supporta lə segnalanti nella stesura di segnalazioni più chiare e precise, ma garantisce anche un'indagine più efficace e approfondita.

2.3 QUADRO GENERALE DELLE PROCEDURE DI INDAGINE

La Direttiva, nel suo Art. 9, Par. 1, stabilisce che la procedura di **segnalazione interna debba includere una gestione accurata della segnalazione (si parla anche di "attento seguito", in traduzione dell'espressione inglese *diligent follow-up*) da parte della persona o del servizio designato a tal fine** (cfr. **capitolo 1**).

A questo proposito, l'Art. 5.12 definisce il "*follow-up*" (seguito) come "*qualsiasi azione intrapresa dal destinatario di una segnalazione o da un'autorità competente al fine di valutare l'accuratezza delle accuse contenute nella segnalazione e, se è il caso, di porre rimedio alla violazione segnalata, anche attraverso azioni quali un'indagine interna, un'investigazione, un'azione penale, un'azione per il recupero di fondi o l'archiviazione della procedura*".

Pertanto, la Direttiva include due azioni nel concetto di gestione accurata della segnalazione: la **valutazione dell'accuratezza** delle questioni segnalate e la **risoluzione della violazione** segnalata.

Secondo la relazione sull'attuazione della Direttiva, **nella maggior parte degli Stati membri diverse componenti dell'articolo 9 non sono state recepite correttamente**: tra queste figurano l'obbligo di fornire un diligente seguito alle segnalazioni, i termini per l'emissione dell'avviso di ricevimento e la previsione di eventuali riunioni in presenza. Le normative nazionali di recepimento prese ad esempio in questa guida stabiliscono generalmente un contenuto minimo e/o principi generali per le procedure di segnalazione interna, senza però disciplinarle in dettaglio. Ne risulta che i soggetti obbligati conservano un certo margine di discrezionalità nell'autoregolamentazione e nell'organizzazione delle indagini interne, purché rispettino i principi e i requisiti minimi previsti dalla legge nazionale. Questo consente di adattare meglio le procedure alle specifiche caratteristiche di ciascuna organizzazione.

Più in dettaglio: in **Italia**, l'art. 4 del decreto legislativo di recepimento del 2023 stabilisce che gli enti pubblici e privati devono istituire canali che garantiscano la riservatezza dell'identità dellə segnalante, delle persone coinvolte o menzionate nella segnalazione, nonché del contenuto della segnalazione e della documentazione allegata, anche mediante strumenti di crittografia.

Anche in **Spagna**, sono stati introdotti requisiti minimi per le procedure interne, tra cui la comunicazione con lə segnalante entro termini prestabiliti e la trasmissione delle informazioni all'autorità giudiziaria in caso di reato. Tuttavia, anche in questi casi le disposizioni sul seguito concreto delle segnalazioni restano parzialmente generiche, lasciando margini di incertezza sull'effettiva attuazione del principio di gestione accurata della segnalazione.

2.3.1 Procedura d'indagine: linee guida, principi e garanzie

Per garantire la certezza del diritto nelle indagini interne e per proteggere i soggetti investigatori stessi (cfr. cap 4), è altamente consigliabile che le procedure di gestione delle segnalazioni interne siano dettagliate e comunicate (cfr. capitolo 1) in modo completo. Al di là del contenuto minimo e dei principi delineati dalle leggi nazionali di recepimento viste sopra, **le procedure interne dovrebbero descrivere esplicitamente ogni fase del processo di gestione delle segnalazioni**, specificando le azioni da eseguire in ciascuna fase. Tali procedure dovrebbero inoltre disciplinare i metodi di verifica e delineare misure adeguate per conservare e salvaguardare la documentazione e gli elementi probatori raccolti nel corso delle indagini.

Le fasi della procedura di segnalazione interna che potrebbero essere incluse nella procedura sono le seguenti:

A. **Fase di ricezione della segnalazione**: La segnalazione viene formalmente ricevuta e registrata. La persona segnalante riceve una conferma di ricezione e la segnalazione viene valutata per determinarne la pertinenza.
B. **Fase di analisi preliminare della segnalazione**: Si valuta se la segnalazione è ammissibile. Se accolta, si avvia l'indagine; se rigettata, chi segnala riceve un'informazione con motivazioni chiare del rigetto.
C. **Fase di indagine**: Si raccolgono prove per verificare la fondatezza delle accuse. L'indagine è imparziale e trasparente, con aggiornamenti periodici a chi ha segnalato, nel rispetto della riservatezza.
D. **Fase di completamento o conclusione dell'azione**: Si redige un rapporto finale e si decidono eventuali azioni correttive. Chi ha segnalato riceve informazione sull'esito della segnalazione, mantenendo la riservatezza delle persone coinvolte.

2.4 I DIRITTI DELLE PERSONE SEGNALANTI NEL QUADRO DELLE INDAGINI

In questo capitolo, la discussione sulle indagini di *whistleblowing* non approfondisce in modo esteso i diritti delle persone segnalanti, trattandosi di un tema affrontato in modo più ampio in altre sezioni della guida (**cfr. capitolo 4**).

Cp. 4>

Tuttavia, è utile richiamare alcuni aspetti essenziali, poiché **tutelare i diritti delle persone segnalanti non è solo un obbligo normativo, ma anche una condizione necessaria per garantire l'efficacia e la correttezza anche dell'intero processo investigativo**.

In particolare, alcuni diritti risultano particolarmente rilevanti quando si entra nella fase dell'indagine:

A. **Il diritto alla riservatezza**, che protegge l'identità della persona segnalante e consente lo svolgimento delle verifiche senza pressioni esterne o ritorsioni.
B. **Il diritto a essere informatə sul contenuto della segnalazione per poter esercitare il diritto di difesa** , che contribuisce a rendere il processo trasparente e tracciabile.

Ci sono poi situazioni non riconosciute formalmente come diritti obbligatori dalla Direttiva, sebbene citate dalla stessa, ma certamente auspicabili:

A. **Il diritto a una consulenza legale gratuita e riservata**, utile per orientarsi fin dall'inizio e comprendere rischi, tutele e canali disponibili.
B. **Il diritto alla protezione da ritorsioni**, comprese forme indirette come demansionamenti, isolamento o diffamazione, che potrebbero compromettere la disponibilità a collaborare.
C. **Il diritto a misure di sostegno, anche psicologico o finanziario**, nei casi in cui le conseguenze dell'indagine si estendano alla sfera personale o professionale della persona segnalante.

Il suggerimento che forniamo nella presente guida è di **non slegare mai il quadro delle indagini da quello dei diritti della persona segnalante, al pari di quelli della persona segnalata**. Includere questi elementi nel disegno delle indagini non è solo una garanzia di correttezza procedurale, ma anche una leva concreta per rafforzare la qualità e l'affidabilità dell'intero sistema.

2.5 STRUTTURA E RESPONSABILITÀ DELL'INFORMATIVA INTERNA

La nomina di una persona responsabile per il canale di segnalazione interna (e, se serve, di un *team* di supporto per gestire le segnalazioni) deve avvenire

in modo trasparente. **Chi potrebbe usare il canale deve sapere chiaramente chi lo gestisce e chi tratterà l'indagine**. Le persone incaricate devono avere competenze tecniche adeguate e saper condurre indagini in modo efficace.

Organizzare così il lavoro non è solo una questione formale: sapere chi gestisce le diverse fasi delle segnalazioni, come viene tutelata la riservatezza e quali competenze vengono messe in campo è essenziale per garantire indagini affidabili, tempestive e imparziali. Questo approccio aumenta la fiducia nel sistema e aiuta a trattare le segnalazioni con serietà fin dall'inizio.

Tuttavia, in tal caso il principio di trasparenza comporta anche delle sfide, in particolare nella creazione di piattaforme di comunicazione efficaci per individui esterni all'organizzazione (per esempio, appaltatori, ex stagistə).

Da un punto di vista pratico, **soprattutto nelle grandi organizzazioni,** potrebbe essere praticamente **impossibile per una singola persona o reparto gestire tutte le segnalazioni interne** inviate attraverso il canale. Inoltre, la Direttiva Art. 16 impone agli Stati membri di garantire che l'identità della persona segnalante non sia divulgata senza il suo esplicito consenso, a eccezione di un membro del personale autorizzato responsabile del trattamento o del seguito delle segnalazioni (Direttiva Art. 5, Par. 12). Questa disposizione implica che un *team* di persone, in possesso della necessaria formazione tecnica e vincolato da rigorosi obblighi di riservatezza, possa essere coinvolto nel monitoraggio delle segnalazioni, nell'analisi dei casi da diverse prospettive o nello svolgimento di diverse funzioni investigative.

Pertanto, **si consiglia di:**

A. **Fare esplicito riferimento all'esistenza del canale di segnalazione nelle clausole contrattuali** o nei documenti integrativi, nel rispetto degli obblighi di trasparenza previsti dalla Direttiva.
B. **Designare preventivamente una persona supplente** che possa sostituire temporaneamente o permanentemente la persona responsabile del canale di segnalazione interna in caso di vacanza, assenza o malattia. Questo meccanismo di sostituzione è essenziale anche nelle situazioni in cui il manager principale del canale debba astenersi a causa di un conflitto d'interessi o di altri motivi legalmente stabiliti.
C. **Informare le persone segnalate** della procedura d'indagine e dell'identità delle persone incaricate di condurre l'indagine interna.

Inoltre, **lə segnalatə devono potersi fidare** nel fatto che le persone designate alla gestione del canale agiranno in modo obiettivo e imparziale. Garantendo che le segnalazioni siano elaborate e analizzate da professionistə neutrali e competenti, le organizzazioni aumenteranno la fiducia e l'efficacia nel sistema di segnalazione interna. Questo, a sua volta, rafforzerà la fiducia di tuttə lə potenziali utenti nel fatto che il canale di segnalazione funzioni in modo corretto e affidabile e che le segnalazioni siano prese sul serio e gestite con diligenza. Tale disposizione è

fondamentale per **garantire l'obiettività e l'imparzialità nelle indagini interne.**

2.5.1 Struttura organizzativa dei sistemi di segnalazione interna

Stante quanto detto circa la trasparenza, l'organo amministrativo o direttivo dell'ente può designare la persona o le persone responsabili della gestione del canale di segnalazione interna e della ricezione e del seguito delle segnalazioni, come avviene ai sensi della legislazione italiana e spagnola. **Affinché il sistema sia efficace e credibile, tutte le segnalazioni devono essere gestite in modo efficiente e diligente all'interno dell'organizzazione stessa.** Questa responsabilità potrebbe ricadere sulla persona responsabile del canale di segnalazione interna. Pertanto, è essenziale che tali persone, in ragione della loro posizione all'interno dell'organizzazione, siano in grado di svolgere le proprie mansioni in modo indipendente e autonomo, senza essere soggette ad alcuna influenza esterna, e con accesso a tutte le risorse personali e materiali necessarie per svolgere il proprio ruolo. Come accennato in precedenza, le circostanze specifiche di ciascuna organizzazione possono giustificare l'assegnazione di questa responsabilità a un gruppo di persone piuttosto che a un singolo individuo. Oltre a beneficiare del processo decisionale collettivo, un gruppo di questo tipo potrebbe anche apportare una prospettiva multidisciplinare alle indagini.

La selezione dellə professionistə appropriatə può variare a seconda del tipo e della struttura dell'ente. Tuttavia, lə responsabili della gestione del canale di segnalazione interna devono impegnarsi a rispettare le normative, l'integrità e i principi e i valori etici dell'organizzazione. **Tali soggetti devono svolgere le loro funzioni in modo indipendente e autonomo e** comunque **evitando conflitti d'interessi**. In definitiva, la credibilità del sistema di segnalazione interna dipende dalla fiducia che lə dipendenti ripongono nellə responsabili della gestione delle segnalazioni. Se lə dipendenti percepiscono che le segnalazioni sono gestite in modo oggettivo ed efficace, saranno più propensə a utilizzare il canale interno.

Negli enti più piccoli, questa potrebbe essere una doppia funzione svolta da unə dipendente che si trova in una posizione adeguata per comunicare direttamente con la direzione dell'ente, per esempio unə responsabile della *compliance* o delle risorse umane, unə responsabile dell'integrità istituzionale, unə responsabile legale o della *privacy*, unə componente dell'*audit*, unə responsabile della revisione contabile.

In generale, lə responsabile del canale interno può incorrere in **responsabilità derivanti dalla gestione e dal corretto funzionamento del sistema interno.** Tali responsabilità possono riguardare il trattamento diligente e il seguito delle segnalazioni, le garanzie di protezione dellə segnalante all'interno dell'organizzazione stessa, nonché il suo comportamento quando deve interagire con le autorità competenti. Inoltre,

in alcuni casi, lə responsabile può incorrere in responsabilità penale se la condotta è tipizzata dalla normativa penale applicabile (per esempio, divulgazione di segreti, reati commessi da pubblici ufficiali).

In ogni caso, è necessario tenere conto degli obblighi stabiliti dalla normativa nazionale di recepimento degli Stati membri ai fini della determinazione delle responsabilità specifiche dei responsabili e dei soggetti gestori del canale interno, caso per caso.

2.5.2 Conflitti di interesse nei sistemi di segnalazione interna

I conflitti di interesse si verificano quando l'imparzialità e l'obiettività delle persone incaricatə di elaborare giudizi professionali sono compromesse da interessi personali o esterni. Come ogni rischio, **anche i conflitti di interesse devono essere gestiti in modo proattivo**.

Per garantire equità e credibilità nelle indagini interne, è fondamentale che il sistema di segnalazione preveda **misure esplicite per identificare, gestire e affrontare tempestivamente i conflitti di interesse che possono coinvolgere lə responsabili dell'indagine**. La gestione reattiva dei conflitti di interesse (cioè agire solo quando il conflitto è già emerso) non è sufficiente e può compromettere l'affidabilità del sistema. È invece essenziale che l'organizzazione stabilisca sin dall'inizio procedure chiare per affrontare queste situazioni, prevenendo che possano minare la fiducia nel canale di segnalazione.

Un esempio di buona prassi è la richiesta di una "**Dichiarazione di assenza di conflitto di interesse**" da parte di soggetti incaricatə delle indagini, che va fatta prima dell'avvio delle stesse. Questa dichiarazione aiuta a garantire che chi investiga non abbia legami personali o professionali che possano influire sulla loro neutralità, rafforzando così la percezione di imparzialità da parte degli utenti del canale.

Inoltre, le indagini devono essere condotte nei tempi necessari e devono durare al massimo tre mesi, salvo casi di particolare complessità, per i quali è prevista una proroga di altri tre mesi. L'adozione della proroga deve avvenire prima della scadenza del primo periodo, con una motivazione chiara riguardo le difficoltà incontrate e il motivo del ritardo. Questo rispetto dei tempi è cruciale, poiché un allungamento ingiustificato delle indagini può minare ulteriormente la credibilità del sistema e la fiducia nei confronti di chi è responsabile del procedimento.

2.5.3 Considerazioni sulla protezione dei dati

La Direttiva Art. 17 stabilisce che qualsiasi trattamento di dati personali effettuato nell'ambito delle indagini di segnalazione interna deve essere conforme al Regolamento (UE) 2016/679 (GDPR) e alla Direttiva (UE) 2016/680. Inoltre, qualsiasi scambio o trasmissione di informazioni da parte delle istituzioni, agenzie od organismi dell'UE deve essere effettuato in

conformità al Regolamento (UE) 2018/1725, che disciplina la protezione dei dati all'interno delle istituzioni dell'Unione Europea.

Un aspetto cruciale che la Direttiva Art. 17 incorpora è il **principio della minimizzazione dei dati, che si applica in modo particolare alle indagini: è fondamentale evitare la raccolta di dati personali non necessari per l'analisi della segnalazione.** Qualora venissero raccolti dati irrilevanti o accidentali, questi devono essere immediatamente eliminati, garantendo che ogni trattamento sia mirato esclusivamente a quanto necessario per le indagini.

Oltre a questi principi europei, è importante considerare la legislazione nazionale che può stabilire regole specifiche relative all'accesso ai dati personali nel contesto del canale interno, del registro delle segnalazioni e dei fascicoli d'indagine. In particolare, le normative nazionali potrebbero anche definire i periodi di conservazione dei dati, che devono essere rispettati per evitare conservazioni eccessive o non giustificate.

È importante ricordare il contenuto dell'Art. 5 del Regolamento (UE) 2016/679[49], che stabilisce che i **principi guida per garantire la legittimità del trattamento dei dati personali** sono il principio di responsabilità proattiva, il principio di liceità, lealtà e trasparenza, il principio di limitazione delle finalità, il principio di minimizzazione dei dati, il principio di esattezza, il principio di limitazione del periodo di conservazione e il principio di integrità e riservatezza. (cfr. **capitolo 3** per leggere i dettagli esaustivi).

2.6 PROCESSO DI INDAGINE NELL'AMBITO DEL SISTEMA DI SEGNALAZIONE INTERNA

Consigliamo di istituire un sistema per l'identificazione delle segnalazioni, insieme a una registrazione delle informazioni ricevute e delle indagini interne condotte. Particolare attenzione deve essere prestata alla limitazione dei periodi di conservazione dei dati personali (cfr. **capitolo 3** per approfondire). Durante la fase di ricezione della segnalazione, **lə segnalante deve ricevere un avviso di ricevimento entro sette giorni**. Questa conferma è essenziale, in quanto **serve come prova che ha inviato una segnalazione** attraverso il canale di segnalazione interno. Può essere

---

[49] *1. Art. 5. I dati personali sono: https://gdpr-info.eu/art-89-gdpr/https://gdpr-info.eu/art-89-gdpr/*
a. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza").
b. Raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità; l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato, ai sensi dell'Art. 89, paragrafo 1, incompatibile con le finalità iniziali ("limitazione delle finalità").
c. Adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati ("minimizzazione dei dati").
d. Accurati e, ove necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per garantire che i dati personali inesatti, tenuto conto delle finalità per le quali sono trattati, siano cancellati o rettificati senza indugio ("esattezza").
e. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi nella misura in cui saranno trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'Art. 89 (1) fatta salva l'attuazione delle misure tecniche e organizzative adeguate richieste dal presente regolamento al fine di salvaguardare i diritti e le libertà dell'interessato ("limitazione della conservazione").
f. Trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentali, utilizzando misure tecniche o organizzative adeguate ("integrità e riservatezza").
2. Lə responsabile del trattamento è responsabile del rispetto del Par. 1 ("responsabilità") ed è in grado di dimostrare il rispetto dello stesso..

richiesto anche quando si richiedono misure di protezione e/o sostegno all'autorità competente.

Una volta ricevuta una segnalazione, la fase successiva di un protocollo di indagine interna potrebbe essere quella di determinare l'**ammissibilità della segnalazione**. Lə responsabile del canale interno deve valutare la segnalazione e decidere, con motivazione, su una delle seguenti opzioni:

A. Inammissibilità della segnalazione.
B. Ammissione della segnalazione per successive indagini .
C. Invio della segnalazione ad autorità competenti per la trattazione del problema segnalato (Procura della Repubblica, Procura della Corte dei Conti, Procura europea o a qualsiasi altra autorità, ente od organismo competente).

Esempi di criteri di inammissibilità

Una segnalazione può essere considerata inammissibile nelle seguenti circostanze:

A. Accuse manifestamente incomprensibili e non plausibili, comprese notizie prima facie false o prive di basi oggettive.
B. Segnalazioni prive di una descrizione minima dei fatti, come l'ora, il luogo o la natura della presunta infrazione o irregolarità.
C. Segnalazioni basate esclusivamente su dicerie, speculazioni, voci o supposizioni.
D. Segnalazioni relative a fatti identici già indagati e risolti dall'organizzazione, a meno che non vengano fornite nuove prove o informazioni significative.

l contenuto della segnalazione è sottoposto alla **verifica della plausibilità:** tutto ciò che non offre alcuna nota o elemento di falsità può essere considerato plausibile. Una segnalazione è considerata **plausibile quando vi sono indizi sufficienti per giustificare ulteriori indagini**. Condurre un'approfondita valutazione della plausibilità è fondamentale per evitare indagini arbitrarie o non necessarie. La plausibilità di una segnalazione deve essere continuamente rivalutata durante tutta la fase di indagine, assicurando che le prove raccolte siano in linea con i fatti riportati. Successivamente, la persona presumibilmente responsabile viene identificata e le prove raccolte.

Per quanto riguarda la prima causa di inammissibilità (false segnalazioni *prima facie*) il Considerando 101 della Direttiva prevede il mantenimento della protezione quando i fatti riportati sono inesatti o fuorvianti ai sensi delle norme del diritto nazionale generale. Tuttavia, l'Art. 23 della stessa impone agli Stati membri di imporre sanzioni in caso di segnalazioni consapevolmente false o dolose, al fine di prevenire nuove segnalazioni false o dolose e preservare la credibilità del sistema. Tali sanzioni devono essere proporzionate e garantire che non creino un effetto deterrente sullə

segnalanti legittimə. In caso di false segnalazioni, gli enti devono rispettare le leggi nazionali di recepimento che disciplinano la materia.

Secondo il Rapporto di attuazione della Direttiva emesso dalla Commissione Europea, **in merito a questo regime sanzionatorio sono stati rilevati alcuni problemi di conformità** riguardanti la normativa nazionale di recepimento, ad esempio i seguenti:

A. Mancanza di certezza giuridica su ciò che costituisce una condotta sanzionabile.
B. Multe inefficaci e basse, riducendo la deterrenza.
C. Sanzione delle ritorsioni solo nei confronti delle persone segnalanti, piuttosto che estendere la protezione ad altre categorie di individui, come lə facilitatorə (Direttiva Art. 4).

Secondo la legge italiana, una segnalazione può essere considerata **inammissibile nei seguenti casi:**

A. In caso di mancanza di dati che costituiscono elementi essenziali delle segnalazioni (es. i fatti segnalati e l'Amministrazione o l'Ente in cui si sono verificati; l'Amministrazione o l'Ente nel cui contesto lavorativo opera lə segnalante e il profilo professionale tenuto da quest'ultimə; una breve descrizione delle modalità con cui lə segnalante è venuto a conoscenza dei fatti segnalati, ecc.).
B. Quando le violazioni segnalate non rientrano nell'ambito materiale definito dalla legge italiana.
C. Quando la persona segnalante non figura tra le persone legalmente autorizzate alla segnalazione.
D. Quando i fatti riportati non si riferiscono all'ambiente di lavoro.

2.6.1 Cosa succede quando la segnalazione viene ammessa al trattamento?

Dopo aver valutato l'ammissibilità della segnalazione, è necessario avviare un'indagine interna. In questa fase può essere opportuno considerare l'adozione di eventuali **misure provvisorie** finalizzate a garantire l'efficacia dell'indagine stessa e a prevenire danni potenzialmente irreparabili. Tali misure devono essere previste nella procedura interna, adottate in modo motivato e solo a seguito di un'**analisi preliminare della loro necessità e proporzionalità**.

2.7 POTERI DI INDAGINE

L'obiettivo principale di un'indagine interna è quello di raccogliere e conservare le prove necessarie per stabilire i fatti e determinare eventuali responsabilità. **Le indagini interne** non hanno la stessa portata o natura giuridica delle indagini giudiziarie, in quanto sono di natura amministrativa. Qualsiasi raccolta di prove **deve rigorosamente evitare l'uso di metodi illegali, sleali o non etici** che violano i diritti e le libertà fondamentali, sia

individuali che collettive[50]. Un'indagine che non rispetta questi limiti può comportare **gravi conseguenze**, tra cui l'invalidazione delle prove ottenute e la potenziale responsabilità penale per coloro che conducono l'indagine. Fondamentalmente, le indagini interne si basano su vari mezzi di verifica, i più comuni sono:

A. Documentazione e/o informazioni che incorporano dati ed evidenze.
B. Interviste con testimoni e con le parti.

Per verificare l'accuratezza dei fatti riportati, **i soggetti investigatori in genere richiedono documenti e rapporti** contenenti i dati necessari come prova.

Queste fonti di dati possono essere classificate in:

A. **Fonti interne**: diverse unità organizzative devono collaborare alle indagini, in quanto possono essere in possesso di documenti preziosi che chiariscono le circostanze del caso.
B. **Fonti aperte**: tra le tante consultabili, suggeriamo le seguenti:
   I. I dati relativi agli appalti pubblici possono essere ottenuti consultando registri e piattaforme e sui portali open data degli enti del settore pubblico, come la Banca Dati Nazionale dei Contratti Pubblici di ANAC in Italia[51].
   II. I dati commerciali possono essere ottenuti nei registri pubblici delle imprese e nei bollettini ufficiali.
   III. I dati provenienti dalle amministrazioni e dagli enti pubblici, come i dati generali, i bilanci o i conti annuali, i funzionari eletti, i dirigenti e il personale, gli organigrammi e altri possono essere trovati sui siti web, portali per la trasparenza e gli open data di questi enti.
   IV. I dati relativi a sovvenzioni e contributi possono essere ottenuti dai registri delle sovvenzioni, dai portali open data di diversi enti e anche dai bollettini ufficiali.
   V. I dati delle liste elettorali possono essere ottenuti anche da fonti aperte.
   VI. Dati provenienti dal registro dei gruppi di interesse.
   VII. Dati provenienti dalle agende di funzionari di alto rango.

Quando si utilizzano fonti aperte, **è fondamentale valutare l'affidabilità delle informazioni**. I dati *open source* devono spesso essere filtrati, convalidati e sottoposti a controlli incrociati per garantire l'accuratezza. **Una buona pratica per preservare la riservatezza** è quella di non richiedere tale documentazione ai dipartimenti o alle unità dell'organizzazione stessa se tali informazioni possono essere ottenute consultando fonti aperte.

2.7.1 Quali sono le raccomandazioni relative al colloquio personale?

[50] *Si raccomanda di consultare la sentenza della CEDU 2017/169399 del 5 settembre, causa Bărbulescu c. Romania (Barculescu II) sul riconoscimento della vita privata nel contesto lavorativo.*

[51] *Si veda: https://dati.anticorruzione.it/superset/dashboard/appalti/*

A. Condurre colloqui con almeno due investigatorə presenti.
B. Prevedere le condizioni di discrezione per l'intervista alle persone e le modalità di documentazione e registrazione dell'intervista, oltre a fornire le informazioni necessarie in merito al trattamento dei loro dati personali secondo le disposizioni del GDPR (Art. 15 e seguenti).
C. La prima persona a essere intervistata sarà di regola la persona segnalante (se non è anonima). Successivamente l'intervista dovrebbe proseguire con persone che possono avere informazioni o che possono essere state testimoni dei fatti o dei comportamenti riportati e, infine, lə eventuali partecipanti e/o responsabili dei fatti.
D. Prevedere se l'intervistatə può partecipare in presenza di unə avvocatə o di un'altra persona (facilitatorə, rappresentante sindacale, ecc.).

2.7.2 Chiusura di un'indagine interna

Un'indagine interna deve essere chiusa quando risulta infondata o priva di riscontri. Se i fatti segnalati sono confermati, le possibili **modalità per concludere l'indagine interna** sono le seguenti:

A. **Comunicazione al dipartimento o all' unità competente** affinché possa adottare misure per risolvere la violazione segnalata, quali, tra le altre, misure disciplinari.
B. **Trasferimento a un'autorità amministrativa competente** quando l'infrazione è confermata.
C. **Trasferimento al Pubblico Ministero e/o ad altra autorità giudiziaria**, quando i fatti segnalati integrano un reato. Se l'eventuale azione penale lede gli interessi finanziari dell'Unione europea, la relazione sarà trasferita alla Procura europea.
D. **Raccomandazioni interne** in caso di rilevamento di cattive pratiche e mancanza di professionalità.

2.7.3 Dall'indagine interna alla Procura della Repubblica

L'obbligo di trasferire le informazioni provenienti da un'indagine interna al pubblico ministero o alle autorità giudiziarie è stato previsto nel recepimento della Direttiva Europea, ma rappresenta un tema controverso in tutti e tre i Paesi presi in esame, in particolare per quanto riguarda le persone giuridiche soggette a responsabilità penale delle società.

In alcuni casi, tale obbligo potrebbe entrare in conflitto con il diritto delle persone giuridiche di non auto-incriminarsi, un principio tutelato internazionale e da quello nazionale dei Paesi in esame. Questo conflitto può rendere più complessi determinati aspetti delle indagini e porre sfide legali aggiuntive. Pertanto, **la procedura di gestione delle segnalazioni dovrebbe prevedere la possibilità di adottare misure per risolvere tali conflitti e determinare il trattamento appropriato per queste situazioni**, che dovrebbero essere inclusi nei processi di miglioramento continuo dell'organizzazione.

Se la procedura non consente una gestione adeguata di tali conflitti, si rischia di compromettere l'efficacia del sistema, che è stato concepito per rafforzare la cultura etica, l'integrità istituzionale e la compliance all'interno dell'organizzazione.

Le raccomandazioni risultanti da un'indagine interna, che potrebbero riguardare aspetti di natura legale o procedurale, hanno vari obiettivi, tra cui:

A. **Sviluppare programmi di formazione o sensibilizzazione** per evitare future violazioni.
B. **Migliorare i processi o i protocolli interni** per garantire una gestione più efficace delle segnalazioni.
C. **Garantire la corretta attuazione delle misure correttive** in risposta a violazioni o irregolarità.
D. **Informare l'organo di controllo della conformità** riguardo all'adesione dell'organizzazione al codice etico o di condotta.

Sia la persona destinataria della segnalazione che la persona segnalante devono essere informate dell'esito dell'indagine. La Direttiva riconosce il diritto della persona segnalante di ricevere aggiornamenti sullo stato della propria segnalazione e di essere informata dei risultati finali dell'indagine.

Consigliamo che la relazione o il documento che conclude le azioni includa le modalità di avvio dell'indagine, l'oggetto dell'indagine, le azioni investigative svolte, chi è intervenuto, la valutazione dell'accuratezza dei fatti, nonché le conclusioni e le proposte che finalizzano il seguito della segnalazione ricevuta, come indicato nella Direttiva, per risolvere la violazione segnalata. In ogni caso, deve essere obiettiva, imparziale, chiara e precisa.

2.8 IL RUOLO DELL'AUTORITÀ ESTERNA PER LA SEGNALAZIONE

2.8.1 L'IMPORTANZA DI CANALI DI SEGNALAZIONE EFFICACI PER I SOGGETTI SEGNALANTI

Le autorità competenti sono tenute, da Direttiva europea, a garantire che **i canali di segnalazione esterna siano indipendenti e autonomi, in grado di trattare le segnalazioni in modo adeguato e tempestivo**. Quando i canali interni non sono disponibili, non funzionano correttamente o quando lə potenziali segnalanti temono ritorsioni, le autorità esterne sono spesso più idonee a gestire e trattare le segnalazioni (cfr. capitolo 4). L'Art. 11 della Direttiva stabilisce che tali canali esterni debbano essere indipendenti e autonomi nella ricezione e nel trattamento delle segnalazioni relative a violazioni della legge. Inoltre, lo stesso articolo e il Considerando 65 precisano che le autorità competenti devono avere la capacità e i poteri necessari per valutare l'accuratezza delle segnalazioni, avviare indagini e adottare misure correttive appropriate. Se necessario, devono anche essere

Cp. 4

in grado di rinviare i casi a un altro organo competente per garantire un seguito adeguato.

2.8.2 Sfide di attuazione e ruolo delle autorità competenti

L'attuazione della Direttiva ha incontrato sfide, in quanto alcuni Stati membri hanno avuto difficoltà a identificare le autorità competenti. Inoltre, **circa la metà degli Stati membri ha recepito in modo errato l'Art. 11, Par. 6**, che delinea gli obblighi per le autorità che ricevono le segnalazioni, ma non la competenza per darvi seguito. Per esempio, alcuni Stati impongono tali obblighi solo a determinate autorità, non garantiscono una trasmissione sicura e tempestiva delle segnalazioni od omettono l'obbligo di informare la persona segnalante.

Quando i canali di segnalazione esterna sono centralizzati, gli Stati membri devono garantire il rispetto dei requisiti di indipendenza e autonomia della Direttiva. Gli Artt. 12 e 18 della Direttiva **stabiliscono criteri rigorosi per i canali di segnalazione esterna,** tra cui la garanzia dell'integrità e della riservatezza delle informazioni, l'archiviazione a lungo termine e l'accessibilità delle segnalazioni scritte e orali, comprese le comunicazioni anonime ove consentito dal diritto nazionale. L'Art. 13 impone alle autorità competenti di **pubblicare informazioni chiare e accessibili** sulle procedure di segnalazione, sui ricorsi, sulla protezione contro le ritorsioni e sulla consulenza riservata allə segnalanti. Inoltre, devono essere effettuate revisioni periodiche ogni tre anni per garantire che le procedure di segnalazione rimangano efficaci. Le autorità competenti non solo gestiscono i canali esterni, ma possono anche imporre sanzioni e svolgere un ruolo fondamentale nella promozione di una cultura che incoraggi il *whistleblowing*, garantendo che coloro che segnalano illeciti non siano stigmatizzati od oggetto di ritorsioni.

2.8.3 Segnalazione simultanea a canali interni ed esterni

Sebbene **la Direttiva** non imponga allə segnalanti di effettuare una segnalazione interna prima di utilizzare canali esterni, **la stessa non affronta esplicitamente le modalità di gestione delle segnalazioni interne ed esterne simultanee.** La questione è stata discussa nel corso della quarta riunione del gruppo di espertə, in cui sono state formulate raccomandazioni agli Stati membri affinché includano disposizioni nelle loro leggi di recepimento:

A. Lə segnalanti devono attendere la scadenza del periodo di tre mesi prima di effettuare una segnalazione esterna.
B. Se scelgono di effettuare una segnalazione esterna prima della scadenza del periodo di tre mesi, devono ritirare la loro segnalazione interna.

Inoltre, le leggi nazionali potrebbero consentire alle autorità di chiedere allə segnalanti il consenso per informare il datore di lavoro in merito alla loro

segnalazione esterna. Tuttavia, lə segnalanti non perderebbero mai la loro protezione per aver seguito queste raccomandazioni.

Secondo la Commissione Europea, in pratica, la segnalazione esterna comporterebbe il ritiro implicito della segnalazione interna. Se il datore di lavoro viene a conoscenza di un'indagine esterna, il canale interno non sarebbe più tenuto a dare seguito alla segnalazione. Tuttavia, l'organizzazione può ancora scegliere di continuare la sua indagine interna. Se le indagini interne ed esterne procedono contemporaneamente, le autorità competenti rimangono obbligate a indagare e a porre rimedio alle violazioni previste dalla Direttiva.

In ogni caso, consigliamo di provvedere anche per via giuridica nei diversi Paesi dell'UE: le leggi di recepimento dovrebbero disciplinare le modalità di gestione del concorso di segnalazioni attraverso il canale interno e il canale esterno quando lə segnalante effettua una segnalazione esterna prima della scadenza del periodo di tre mesi per l'indagine interna, a seguito delle raccomandazioni formulate dal gruppo di espertə.

2.9 RACCOMANDAZIONI

1. PRESERVAZIONE DELLA RISERVATEZZA

Devono essere implementate misure procedurali, tecniche, organizzative e di sicurezza per preservare la riservatezza dei dati personali contenuti nei canali di segnalazione interna. Particolare attenzione deve essere posta sulla garanzia e la salvaguardia della riservatezza dell'identità sia della persona segnalante che delle persone segnalate. Le indagini interne devono inoltre essere condotte in modo da ridurre al minimo il rischio di violazioni della riservatezza durante l'intero processo.

2. PROCEDURE DI MONITORAGGIO

Le procedure di gestione e monitoraggio delle segnalazioni interne devono essere dettagliate e indirizzate, oltre ai contenuti minimi e ai principi previsti dalle leggi di recepimento, alle diverse fasi della procedura di indagine nel modo più completo possibile e specificando le azioni da svolgere in ciascuna di esse. Dovrebbero anche stabilire quali saranno i mezzi di verifica.

3. IDENTIFICAZIONE DEL SEGNALETTO

Deve essere presente un **sistema di identificazione delle segnalazioni, insieme a un registro** delle segnalazioni ricevute e delle indagini condotte. Ciò garantisce la tracciabilità delle operazioni del canale interno e migliora l'*accountability*.

4. DETERMINARE L'AMMISSIBILITÀ

La procedura di gestione delle segnalazioni deve **definire le circostanze in cui una segnalazione sarà considerata inammissibile.**

5. INDAGINI INTERNE PIANIFICATE

Le indagini interne devono essere adeguatamente pianificate, con una tempistica chiara per evitare ritardi ingiustificati che potrebbero superare il periodo di tempo designato. Il piano dovrebbe definire:

A. L'ambito dell'indagine.
B. Fonti di prova e documentazione richiesta.
C. Le persone coinvolte e quelle che dovrebbero essere intervistate.

6. LIMITI PROVVISORI

La raccolta delle prove nell'ambito delle indagini interne deve rispettare i limiti probatori e, in ogni caso, deve rispettare i diritti e i principi fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'UE, nonché le disposizioni del diritto nazionale e le procedure e i protocolli interni approvati dall'organizzazione.

7. RIDUZIONE AL MINIMO DELLE RICHIESTE DI DOCUMENTI E RICORDO DELLA RISERVATEZZA

Non richiedere documentazione all'organizzazione se tali dati possono essere ottenuti da fonti aperte (per esempio, la nomina di unə dipendente pubblicə pubblicata nella gazzetta ufficiale), **ricordando** altresì alle persone intervistate o ai settori alle quali devono essere richieste le informazioni e/o la documentazione **gli obblighi di riservatezza e le conseguenze** che una violazione della riservatezza può comportare.

8. MOTIVAZIONE DELLA RACCOLTA DELLE PROVE NELLE RELAZIONI

La relazione d'indagine deve includere una motivazione per le azioni e i metodi di verifica utilizzati per raccogliere le prove.

9. PIANIFICAZIONE E DOCUMENTAZIONE DELLE INTERVISTE

Nella fase di pianificazione delle indagini, è necessario **determinare i criteri per decidere quali persone debbano essere sentite e in quale ordine,** nonché prevedere le condizioni di discrezione per farlo e le modalità di documentazione e registrazione dell'interrogatorio. Si consiglia che venga eseguito da due investigatorə.

10. STRUTTURA DEL RAPPORTO FINALE DI INDAGINE

La relazione che conclude l'indagine deve includere una serie di elementi: le modalità di avvio dell'indagine, gli obiettivi dell'indagine, le

azioni intraprese e le persone coinvolte, la valutazione dell'accuratezza dei fatti, le conclusioni e le raccomandazioni per risolvere la violazione segnalata.

11. GARANTIRE OBIETTIVITÀ E CHIAREZZA NELLE SEGNALAZIONI

Il rapporto finale deve essere **obiettivo, imparziale, chiaro e preciso.**

12. GESTIONE DEI CONFLITTI DI INTERESSE NEL *FOLLOW-UP*

La procedura di seguito deve includere **meccanismi per identificare, gestire e mitigare i conflitti d'interessi** tra lə responsabili della gestione delle segnalazioni.

13. RACCOMANDAZIONI PER IL MIGLIORAMENTO ORGANIZZATIVO

La procedura di gestione delle segnalazioni deve prevedere la **possibilità di emettere raccomandazioni** per determinare il trattamento che le situazioni rilevate di cattive pratiche e di mancanza di professionalità (illeciti) meritano e da inserire nei processi di miglioramento continuo dell'organizzazione.

14. PROROGA DEI TERMINI DI INDAGINE

Se un'indagine non può essere completata entro il periodo iniziale di tre mesi, può essere concessa un'ulteriore **proroga di tre mesi.** Tuttavia, questa proroga deve essere approvata prima della fine del primo periodo, giustificare il motivo del ritardo e specificare le azioni in sospeso da completare.

15. PROMOZIONE DI UNA CULTURA DEL *WISTLEBLOWING*

Le autorità competenti devono **promuovere una cultura del *whistleblowing*.**

16. GESTIONE DELLE SEGNALAZIONI ESTERNE PRECOCI

Le leggi di recepimento devono **chiarire come gestire i casi in cui unə segnalante effettua una segnalazione esterna prima della scadenza del periodo di tre mesi dell'indagine interna.** Ciò deve essere in linea con le raccomandazioni del gruppo di espertə della Commissione Europea.

17. SANZIONI PER VIOLAZIONI DELLA RISERVATEZZA

Devono esserci **sanzioni dissuasive ed efficaci in caso di inosservanza dell'obbligo di riservatezza** che affrontano specificamente la violazione di questa disposizione della Direttiva. Pertanto, in caso di violazione della riservatezza e dell'obbligo di segretezza, sarà necessario considerare i reati tipizzati dalle leggi di recepimento degli Stati membri.

Protezione dei dati personali

Capitolo 3

Open the whistle

PROTEZIONE DEI DATI PERSONALI

Capitolo 3

3.1 IL RUOLO DELLA PROTEZIONE DEI DATI NEI SISTEMI DI *WHISTLEBLOWING*

Nel capitolo seguente di questa guida, affronteremo un altro aspetto che risulta tanto cruciale quanto problematico, se si parla di *whistleblowing*: la protezione dei dati personali. Proveremo a inquadrare la questione e, parimenti, a suggerire alcune indicazioni **pratiche che facilitino il rispetto della *privacy*, evitando interpretazioni che la trasformino in uno svantaggio** per chi segnala e per il funzionamento dell'istituto stesso, anziché in una garanzia. Fare in modo che i principi di protezione dei dati siano rispettati, salvaguardando al contempo la riservatezza e i diritti dellə segnalanti, è infatti essenziale per mantenere la conformità legale. Al tempo stesso, se implementate in modo ponderato, **le misure di protezione dei dati possono promuovere una cultura della fiducia,** migliorare la trasparenza e garantire l'integrità dei sistemi di segnalazione interna.

La prima indispensabile premessa da fare è che, a seconda del tipo di segnalazione, il processo di *whistleblowing* comporta la raccolta, l'uso e la divulgazione (limitata e circostanziata) di dati personali, collocandoli all'intersezione tra i quadri normativi in materia di protezione dei dati e protezione dellə segnalanti. **La protezione dei dati non è solo un obbligo normativo, ma uno strumento progettato per supportare,** servire e soddisfare le esigenze di tutte le parti coinvolte nel processo di *whistleblowing*, considerando quanto il principio di riservatezza sia centrale nell'istituto. Lungi dall'essere un ostacolo ai flussi di lavoro organizzativi, solidi quadri di protezione dei dati **forniscono chiarezza e struttura,** garantendo che lə segnalanti si sentano sicurə nel segnalare comportamenti scorretti e nel chiedere aiuto ai servizi di supporto, salvaguardando al contempo gli interessi delle organizzazioni che ricevono e gestiscono tali segnalazioni.

Il GDPR (Regolamento generale sulla protezione dei dati - Regolamento (UE) 2016/679), in quanto **pietra angolare della protezione dei dati nell'Unione Europea,** stabilisce il quadro giuridico per il trattamento dei dati personali e per bilanciare i diritti e gli obblighi di tutte le parti interessate (cfr. **capitolo 1** per la differenza tra anonimato e riservatezza). Le sfide specifiche del trattamento dei dati sensibili e personali nei contesti di *whistleblowing* sottolineano l'importanza di allineare le strategie di protezione dei dati ai requisiti della Direttiva sulla protezione dei soggetti segnalanti. A livello nazionale, i quadri per la protezione dei dati nei sistemi di *whistleblowing* richiedono una pianificazione meticolosa e un allineamento strategico con i contesti giuridici e culturali nazionali.

Cp. 1 >

Le Nazioni Unite (ONU) sottolineano l'importanza di proteggere lə segnalanti dalle ritorsioni come pietra angolare della trasparenza e dell'*accountability*[52]. I meccanismi di *whistleblowing* devono dare priorità alla riservatezza degli individui per prevenire qualsiasi forma di ritorsione. Ciò include la progettazione di canali di segnalazione sicuri, la garanzia dell'anonimato e l'adozione di tecnologie come la crittografia per proteggere i dati sensibili. La ***policy* delle Nazioni Unite "Protezione contro le ritorsioni"** illustra il ruolo fondamentale della sicurezza dei dati nel promuovere una cultura in cui le persone si sentano sicure di segnalare illeciti senza timore di danni personali o professionali.

3.2 CONCETTO PRINCIPALE E PRINCIPI CHIAVE DELLA PROTEZIONE DEI DATI

L'interazione tra il **Regolamento (UE) 2016/679 (GDPR)** sulla protezione dei dati e la **Direttiva (UE) 2019/1937** sul *whistleblowing* stabilisce il quadro giuridico **per garantire che i dati personali siano trattati in modo lecito, etico e** trasparente. Quando i principi di protezione dei dati sono integrati nella progettazione dei meccanismi di *whistleblowing*, ne migliorano la credibilità e garantiscono il rispetto degli standard legali ed etici.

3.2.1 Perché la protezione dei dati è essenziale per la protezione delle persone segnalanti?

La protezione dei dati risulta essenziale perché:

A. **Salvaguarda le informazioni personali**, sensibili e riservate da uso improprio, furto, accesso non autorizzato, ecc.
B. **Preserva la privacy individuale** garantendo il controllo sui dati personali, riducendo il rischio di danni o sfruttamento.
C. **Previene il furto di identità e le frodi**, considerando che le violazioni che espongono informazioni sensibili possono avere conseguenze devastanti. Le aziende inoltre guadagnano fiducia dando priorità alla protezione dei dati, che rafforza le relazioni con clienti e partner della protezione dei dati, poiché la non conformità può portare a multe severe e danni alla reputazione.

Al di là di questi vantaggi pratici, **la protezione dei dati è una responsabilità etica,** che promuove l'equità e la trasparenza nel modo in cui le informazioni vengono gestite. In un mondo interconnesso, una solida sicurezza dei dati mitiga anche le minacce alla sicurezza informatica, dando priorità alla protezione dei dati, gli individui e le organizzazioni creano un ambiente più sicuro e affidabile.

---

[52] *Protezione contro le ritorsioni: https://www.un.org/en/ethics/protection-against-retaliation/index.shtml#:~:text=The%20UN's%20protection%20against%20retaliation,by%20any%20person%20that%20is*

3.2.2 Principi fondamentali della protezione dei dati

In questa guida, suggeriamo di prendere a riferimento i principi stabiliti nel GDPR Art. 5[53] che sono a fondamento della protezione dei dati. **Richiamarsi ai principi aiuta a evitare una lettura meramente formale della *privacy*,** riducendola a un adempimento anziché riconoscerla come garanzia attiva.

Essi sono il punto di partenza per garantire il rispetto delle norme sulla protezione dei dati e garantire un ambiente equo, trasparente e sicuro per le operazioni di trattamento dei dati:

A. **Il principio di liceità, correttezza e trasparenza** sottolinea l'importanza di un trattamento dei dati personali conforme alla legge e rispettoso dei diritti dei soggetti interessati. Nel contesto del *whistleblowing*, la liceità impone alle organizzazioni di garantire una base giuridica per il trattamento dei dati, come il rispetto di un obbligo legale o il perseguimento di interessi legittimi, come l'indagine su comportamenti scorretti. I dati dovrebbero inoltre essere trattati in modo equo, garantendo la trasparenza, il che richiederebbe alle organizzazioni di informare lə segnalanti su come i loro dati saranno raccolti, utilizzati, conservati e potenzialmente condivisi, assicurandosi che comprendano le implicazioni della loro divulgazione.
B. **Il principio di limitazione delle finalità** impone che i dati personali raccolti attraverso i canali di *whistleblowing* debbano essere utilizzati solo per gli scopi specifici per i quali sono stati raccolti. Per esempio, se unə segnalante segnala accuse di frode, le informazioni fornite devono essere utilizzate esclusivamente per indagare sul problema segnalato e non per scopi non correlati come, per esempio, valutare le prestazioni lavorative dellə segnalante. Questo principio protegge dall'uso improprio dei dati e garantisce che i diritti dellə segnalanti e delle altre persone coinvolte non siano ingiustamente compromessi.
C. **La minimizzazione dei dati** è un principio chiave che sottolinea la necessità di raccogliere solo i dati strettamente necessari per l'indagine sulla questione segnalata. Un'eccessiva raccolta di dati non solo aumenta il rischio di violazioni o usi impropri, ma può anche ridurre la fiducia che lə segnalanti ripongono nella riservatezza del processo di segnalazione. Per esempio, i dettagli su terze parti o l'identità dellə segnalante devono essere divulgati solo quando assolutamente necessari per l'indagine e in conformità con le leggi applicabili.
D. **Il principio di accuratezza** garantisce che tutti i dati personali trattati nell'ambito del *whistleblowing* siano corretti e aggiornati. Dati imprecisi possono portare a risultati ingiusti, come accuse infondate o la conclusione errata delle indagini. Le organizzazioni devono attuare procedure per verificare l'accuratezza delle informazioni fornite dallə segnalanti e per rettificare tempestivamente le inesattezze se vengono identificate.
E. **La limitazione della conservazione** richiede che i dati personali siano conservati solo per il tempo necessario a soddisfare lo scopo per il quale sono stati raccolti. Nei casi di *whistleblowing*, ciò significa che i dati devono essere conservati solo per la durata dell'indagine e di eventuali

[53] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

successivi procedimenti legali o amministrativi. La conservazione dei dati a tempo indeterminato potrebbe esporre le persone a rischi eccessivi, come violazioni o uso improprio, e contravvenire ai principi stabiliti in materia di protezione dei dati.

F. **I principi di integrità e riservatezza** previsti dal GDPR sono di fondamentale importanza, per esempio quando nel caso della segnalante possono essere fornite informazioni altamente sensibili, ed è responsabilità delle organizzazioni garantire che tali dati siano sicuri. Misure solide come la crittografia, i controlli di accesso e i canali di segnalazione sicuri sono essenziali per prevenire l'accesso non autorizzato, le violazioni dei dati e altri rischi che potrebbero compromettere la riservatezza dei segnalanti o l'integrità delle indagini.

G. **Il principio di responsabilità** impone alle organizzazioni di dimostrare la conformità alle leggi sulla protezione dei dati nella gestione dei casi di *whistleblowing*. Ciò comporta la conservazione dei registri delle attività di trattamento dei dati, l'esecuzione di valutazioni d'impatto sulla protezione dei dati per i sistemi di *whistleblowing* e la garanzia che tutte le terze parti coinvolte nell'indagine, come revisori esterni o investigatori, rispettino le normative pertinenti in materia di protezione dei dati. Il GDPR tiene conto degli obblighi di riservatezza stabiliti in altri atti giuridici a livello sia nazionale che dell'UE e prevede che debba essere contabilizzato solo il tipo di dati e non i dati stessi.

Oltre a questi principi fondamentali, la protezione di chi segnala deve tenere conto anche di considerazioni specifiche quali l'anonimato, la riservatezza, l'equilibrio dei diritti tra chi segnala e le parti implicate e i trasferimenti transfrontalieri di dati.

Le organizzazioni devono bilanciare la riservatezza del soggetto segnalante con i diritti delle persone coinvolte di accedere alle informazioni relative alle contestazioni nei loro confronti, garantendo che ciò avvenga in conformità con i requisiti legali. Quando il *whistleblowing* coinvolge questioni internazionali, le organizzazioni devono garantire che qualsiasi trasferimento transfrontaliero di dati sia conforme alle normative applicabili, come il GDPR nell'UE.

È fondamentale aderire a questi principi in modo che le organizzazioni possano proteggere i diritti di tutte le parti coinvolte, garantire il rispetto dei quadri giuridici e promuovere una cultura di responsabilità e trasparenza nei sistemi di protezione di segnalanti e contribuire a coltivare la fiducia.

3.3. BASE GIURIDICA PER IL TRATTAMENTO LECITO DEI DATI PERSONALI

Art. 6 del GDPR

Le organizzazioni coinvolte nei processi di *whistleblowing* devono identificare una base giuridica per il trattamento dei dati personali come indicato nell'Art. 6 del GDPR[54]. Le basi giuridiche del trattamento includono

[54] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

il consenso, l'obbligo contrattuale, l'obbligo legale, gli interessi vitali, l'interesse pubblico e gli interessi legittimi:

A. **Il consenso** prevede che il trattamento dei dati personali sia lecito quando l'interessato ha dato un consenso libero, specifico, informato e inequivocabile al trattamento dei propri dati per una determinata finalità. Il consenso deve essere chiaro, esplicito (in caso di trattamento di dati sensibili) e facilmente revocabile in qualsiasi momento.
B. **La base dell'obbligo contrattuale** si applica quando il trattamento è necessario per l'adempimento di un contratto di cui l'interessatə è parte o per l'esecuzione di misure precontrattuali su richiesta dell'interessatə. Ciò garantisce che il trattamento dei dati sia direttamente collegato all'adempimento o alla preparazione di un obbligo contrattuale (la protezione dei soggetti segnalanti può far parte delle disposizioni di qualsiasi contratto).
C. **L'obbligo legale** è lecito quando è necessario per adempiere a uno specifico requisito legale imposto al titolare del trattamento. Questa base giuridica è generalmente utilizzata quando la legislazione impone la conservazione, la segnalazione o la condivisione dei dati (ai sensi degli atti legislativi, come la Direttiva europea e il diritto nazionale, la protezione dellə segnalanti è soggetta agli obblighi legali applicabili alle organizzazioni).
D. **La base giuridica degli interessi vitali** giustifica il trattamento quando è necessario per proteggere la vita o la sicurezza fisica dell'interessatə o di un'altra persona. Questa base è spesso utilizzata in caso di emergenza, come le situazioni mediche, in cui non è possibile ottenere il consenso.
E. **L'interesse pubblico** o la base giuridica dell'autorità pubblica si applica quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Questo è comunemente utilizzato da enti pubblici o organizzazioni che operano in base a mandati statutari o governativi, mentre dovrebbe essere esplicitamente indicato nell'atto giuridico specifico.
F. **Interessi legittimi**: il trattamento è lecito quando è necessario per raggiungere gli interessi legittimi del titolare del trattamento o di un terzo, a condizione che su tali interessi non prevalgano i diritti e le libertà della persona interessata. Tale base giuridica richiede un attento bilanciamento per garantire che il trattamento non incida ingiustamente sulla privacy della persona interessata (sebbene la scelta della base giuridica più appropriata sia nelle mani delle organizzazioni, quando possibile, si raccomanda di fare riferimento a quanto previsto dall'Art. 6 del GDPR).

In sintesi, il trattamento lecito dei dati personali ai sensi del GDPR Art. 6 è essenziale per garantire la conformità e promuovere la fiducia nei meccanismi di *whistleblowing*. Le organizzazioni devono determinare e documentare attentamente la base giuridica appropriata, bilanciando nel contempo i diritti dellə interessatə e i requisiti previsti dalla Direttiva.

Art. 9 del GDPR

Categorie speciali di dati personali, comprese le informazioni relative all'origine razziale[55] o etnica, alle opinioni politiche, alle convinzioni religiose, alla salute o all'orientamento sessuale, **sono soggette a protezioni rafforzate ai sensi dell'Art. 9 del GDPR[56]**. Queste tipologie di dati sono considerate sensibili e richiedono specifiche condizioni per giustificarne il trattamento. Il consenso esplicito rimane una condizione primaria per il trattamento dei dati sensibili, ma le organizzazioni devono garantire che tale consenso sia dato liberamente e ben documentato.

FOCUS GENERE

Integrando le politiche sensibili al genere nei quadri di protezione dei dati, i sistemi di *whistleblowing* possono diventare più sicuri ed efficaci, incoraggiando un maggior numero di persone, in particolare le donne, a farsi avanti senza timore di ritorsioni o esposizioni. Queste misure sono essenziali per **garantire che le segnalazioni di comportamenti scorretti con un impatto di genere siano gestite in modo sicuro** e che l'identità di potenziali segnalanti rimanga protetta, soprattutto quando ci sono dinamiche di potere che potrebbero influenzare il processo. Si consiglia di:

A. **Sottolineare come i sistemi di sicurezza prevengano le ritorsioni nei casi basati sul genere**, garantendo che le segnalazioni siano protette dall'accesso da parte di individui nella stessa gerarchia sul posto di lavoro, come supervisori o colleghi, per evitare potenziali ritorsioni.
B. **Garantire che le piattaforme che rivendicano l'anonimato proteggano realmente l'identità del segnalante**, in particolare nei casi che coinvolgono squilibri di genere e di potere intersezionale (per esempio, datore di lavoro-dipendente, professorə-studentə, governo-cittadinə).
C. **Fornire informazioni esplicite su come le misure di sicurezza digitale** (per esempio, TOR, protocolli a conoscenza zero, mascheramento IP) proteggono lə segnalanti che segnalano comportamenti scorretti basati sul genere.
D. Sviluppare piattaforme *online* e linee telefoniche dirette per la segnalazione, consentendo alle persone di effettuare segnalazioni da casa e, in alcuni casi, in modo anonimo. Questo modo di segnalare **può essere particolarmente utile per segnalare la violenza di genere** legata alla corruzione e alla *sextortion*.

Protocolli di riservatezza per le segnalazioni basate sul genere:

A. Specificare **ulteriori tutele di riservatezza per lə segnalanti che segnalano comportamenti scorretti basati con un impatto di genere**, comprese misure per impedire l'identificazione indiretta attraverso i dettagli del caso.
B. Spiegare in dettaglio come le **segnalazioni di violenza di genere saranno archiviate in modo sicuro** e separate dalle segnalazioni di cattiva condotta generale per ridurre al minimo l'esposizione.
C. **Chiarire chi ha accesso alle segnalazioni e come viene applicata la protezione dell'identità,** garantendo che nessuna persona non autorizzata (per esempio, colleghə o superiori diretti) possa accedere ai dati sensibili.

La riservatezza è fondamentale per mantenere l'integrità delle segnalazioni di comportamenti scorretti basati sul genere e proteggere lə segnalanti da potenziali danni.

[55] *È la terminologia usata nel GDPR.*

[56] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Altre basi giuridiche per il trattamento dei dati sensibili includono il rispetto degli obblighi di legge, la necessità del trattamento per un interesse pubblico sostanziale e la protezione di interessi vitali. Per esempio, i casi di *whistleblowing* che comportano accuse di discriminazione possono richiedere il trattamento di dati sensibili per comprovare le segnalazioni o rispettare le leggi antidiscriminazione. Le organizzazioni devono prestare attenzione e implementare ulteriori misure di sicurezza durante la gestione di tali dati per mitigare i rischi e garantire la conformità.

Diritti degli interessati ai sensi del Regolamento (UE) 2016/79 (GDPR)

Il GDPR concede agli interessati una serie di diritti volti a responsabilizzare le persone e a fornire un maggiore controllo sui loro dati personali. Tra questi ci sono:

A. **Il diritto di accesso**, che consente alle persone di ottenere informazioni dettagliate sul trattamento dei propri dati, comprese le finalità, le categorie, i destinatari e i periodi di conservazione.
B. **Il diritto di rettifica**, che garantisce che i dati inesatti o incompleti possano essere corretti tempestivamente, migliorando l'accuratezza e l'affidabilità delle informazioni trattate.
C. **Il diritto di richiedere** la cancellazione dei dati in circostanze specifiche, ad esempio quando i dati non sono più necessari per la loro finalità originaria o quando il consenso viene revocato. Tuttavia, questo diritto non è assoluto e deve essere bilanciato con la necessità di conservare i dati per scopi legali o investigativi.
D. **Il diritto di limitare il trattamento**, che consente alle persone di limitare l'ambito delle attività di trattamento dei dati, in particolare durante le controversie sull'accuratezza o sulla liceità del trattamento.
E. **Portabilità dei dati**, che consente alle persone di ricevere i propri dati in un formato strutturato, di uso comune e leggibile da una macchina e di trasferirli a un altro titolare del trattamento. Questo diritto rafforza l'autonomia individuale e facilita la concorrenza tra i prestatori di servizi.
F. **Il diritto di opposizione**, che consente alle persone di opporsi alle attività di trattamento dei dati sulla base di interessi legittimi o motivi di interesse pubblico. Le organizzazioni devono valutare attentamente tali obiezioni e fornire giustificazioni chiare per continuare o cessare le attività di trattamento.

Ogni Paese determina le procedure specifiche per l'esercizio dei diritti dellə interessatə ai sensi del GDPR Artt. da 15 a 22[57], che di solito includono una richiesta al titolare del trattamento per l'esercizio dei propri diritti. **La legislazione nazionale stabilisce se tali richieste debbano essere presentate per via elettronica, per iscritto o in entrambi i modi,** o attraverso un metodo specifico per l'organizzazione, che non dovrebbe creare ulteriori difficoltà allə interessatə, né superare in modo sproporzionato l'onere amministrativo per il titolare del trattamento.

[57] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

3.6. INTERAZIONE TRA IL QUADRO GIURIDICO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LA DIRETTIVA (UE) 2019/1937

Anche se il GDPR riconosce a tutte le figure coinvolte nel *whistleblowing* una serie di diritti, è importante considerare sempre la sua interazione con le altre normative applicabili. Quando una persona è considerata segnalante ai sensi della Direttiva (UE) 2019/1937, può comunque esercitare tutti i diritti previsti dal GDPR. Tuttavia, **le organizzazioni possono rifiutarsi di dare seguito a queste richieste**, o di soddisfarle pienamente, se ciò comportasse una violazione dei requisiti legali per la protezione dellə segnalante, quando ciò va a costituire una violazione dei requisiti legali per la protezione dellə segnalanti ai sensi della Direttiva e del diritto nazionale.

A riguardo, il GDPR stabilisce requisiti e tempistiche per la cancellazione dei dati personali, sia al completamento dello scopo per cui sono stati raccolti, sia su richiesta dellə interessatə. In questo contesto, **il Regolamento sulla *privacy* si applica come *lex generalis***: ciò significa che, se la normativa nazionale prevede periodi di conservazione differenti in base alla tipologia di dati o al procedimento, queste disposizioni prevalgono. Infine, **le organizzazioni possono ancora basare il trattamento dei dati sull'interesse legittimo, ma in questi casi devono essere in grado di dimostrarlo** con elementi concreti e documentati e prove sufficienti.

In questa guida, sosteniamo come entrambi i quadri condividano l'obiettivo comune di promuovere la trasparenza e l'*accountability*, salvaguardando nel contempo i diritti delle persone. La gestione riservata delle segnalazioni di irregolarità è un requisito fondamentale ai sensi della Direttiva e del GDPR. **Entrambi i quadri impongono che siano raccolti e trattati solo i dati necessari per conseguire le finalità del meccanismo di segnalazione**. Ciò riduce i rischi associati alla raccolta eccessiva e garantisce il rispetto del principio della limitazione delle finalità. I dati devono essere conservati solo per il tempo necessario a indagare e risolvere i problemi segnalati.

In Italia, il diritto nazionale applicabile prevede che le segnalazioni non possano essere utilizzate al di là di quanto necessario per dare loro un seguito adeguato. L'identità della persona segnalante e qualsiasi altra informazione da cui tale identità possa essere dedotta, direttamente o indirettamente, non possono essere rivelate, senza il loro esplicito consenso, a soggetti diversi da quelli competenti a ricevere le segnalazioni o a darvi seguito, espressamente autorizzati a trattare tali dati ai sensi degli Artt.t. 29 e 32, Par. 4, del GDPR[58]. Si prevede, inoltre, che i dati personali manifestamente non utili per l'elaborazione di una specifica segnalazione non siano raccolti o, se raccolti accidentalmente, siano cancellati immediatamente (Art. 13.2). Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento

[58] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

della segnalazione e comunque non oltre cinque anni dalla data di comunicazione dell'esito finale della procedura.

Enti pubblici e privati definiscono il proprio modello di ricezione e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati. Inoltre, **la normativa italiana in materia di protezione dei dati personali include una specifica disposizione a tutela della riservatezza dell'identità del segnalante** (Art. 2-undecies del D.Lgs. 196/2003). Tale articolo è stato introdotto con il D.Lgs. 101/2018, per ottemperare al GDPR. La citata disposizione stabilisce che nell'ambito di una segnalazione, il soggetto interessato, presunto autore della violazione, con riferimento ai propri dati personali trattati dall'Amministrazione, non può esercitare i diritti previsti dagli Artt. da 15 a 22 del GDPR, in quanto l'esercizio di tali diritti potrebbe comportare un danno alla tutela della riservatezza dell'identità della persona segnalante. La legge prevede la possibilità per l'interessatə di richiedere all'Autorità Garante per la protezione dei dati personali verifiche sulla conformità del trattamento dei propri dati. Il Garante per la protezione dei dati personali fornisce riscontro sul relativo esito.

Allineando le strategie di protezione dei dati ai requisiti della Direttiva:

A. **Le organizzazioni possono creare sistemi integrati** che rispettino i diritti individuali, supportando al contempo una *governance* e una compliance efficaci. Lə segnalanti si sentono sicurə di farsi avanti, sapendo che i loro dati personali saranno trattati con la massima cura.
B. **La fiducia del pubblico nei sistemi di segnalazione è rafforzata**.
C. **Le autorità di regolamentazione e le organizzazioni devono lavorare in modo collaborativo** per garantire un'implementazione senza soluzione di continuità, sfruttando strumenti come protocolli di segnalazione standardizzati, linee guida chiare sulla conservazione dei dati e tecniche di anonimizzazione accessibili.

3.8 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA NEI CANALI DI SEGNALAZIONE INTERNA

Le organizzazioni possono creare solidi sistemi di *whistleblowing* in linea con i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita.

3.8.1 Che cos'è la protezione dei dati fin dalla progettazione?

Nel caso del canale di segnalazione interno, le misure di sicurezza e le considerazioni sulla *privacy* possono essere integrate nello sviluppo dei meccanismi di segnalazione. Per esempio, i sistemi dovrebbero includere funzionalità come canali di comunicazione crittografati, controlli degli

Cp. 2›

accessi basati sui ruoli e registri di controllo per garantire riservatezza e *accountability*. La **minimizzazione dei dati** (cfr. capitolo 2) **dovrebbe guidare la progettazione dei moduli di segnalazione** e dei flussi di lavoro, garantendo che durante la segnalazione iniziale vengano raccolte solo le informazioni essenziali. Le organizzazioni dovrebbero inoltre attuare procedure per verificare l'accuratezza e la pertinenza dei dati raccolti, salvaguardando nel contempo l'anonimato dei soggetti segnalanti. Un esempio potrebbe essere lo sviluppo di meccanismi interni che consentano il **controllo incrociato di tipi specifici di dati, senza rivelare l'identità del segnalante, al fine di dimostrare la validità** delle affermazioni contenute nelle segnalazioni presentate. Esistono già soluzioni *software* esistenti (compresi quelli utilizzati dagli analisti di dati) che consentono a diversi *database* (settori specifici, risorse umane, ecc.) di effettuare controlli incrociati di tali informazioni in formato anonimo.

L'implementazione di sistemi *software* che incorporano una crittografia robusta per garantire la riservatezza attraverso i canali di segnalazione esterni è un punto di riferimento per un'efficace protezione dei dati fin dalla progettazione. **Un caso di studio dall'Italia è *Globaleaks***, che crea un identificatore per ogni segnalante, consentendo una comunicazione asincrona e sicura con il canale di segnalazione. Tale pratica garantisce che nessuna delle parti possa accedere ai dati personali non necessari, soddisfacendo così il principio della minimizzazione dei dati.

3.8.2 Che cos'è la protezione dei dati per impostazione predefinita?

Con "protezione dei dati per impostazione predefinita" **si intende la necessità per le organizzazioni di elaborare solo i dati necessari per scopi specifici**. I sistemi di segnalazione interni devono applicare automaticamente le impostazioni di *privacy* più elevate e limitare l'accesso ai dati al personale designato. Valutazioni periodiche delle configurazioni e delle pratiche di sistema garantiscono che questi principi siano applicati e aggiornati in modo coerente per affrontare i rischi emergenti e le modifiche normative. Per rafforzare la protezione dei dati, le organizzazioni dovrebbero adottare tecnologie innovative, come i controlli di conformità automatizzati, il rilevamento delle anomalie in tempo reale nei flussi di dati e le soluzioni di archiviazione crittografate (crf. capitolo 1 per ulteriori informazioni). L'interazione con lə dipendenti attraverso corsi di formazione sulla protezione dei dati e sui sistemi di segnalazione interni può colmare il divario tra tecnologia e applicazione pratica. Questo approccio olistico garantisce che il personale a tutti i livelli comprenda le proprie responsabilità, promuovendo una cultura della protezione proattiva dei dati.

Cp. 1›

3.9. PROTEZIONE DEI DATI NEI CANALI DI SEGNALAZIONE ESTERNI

I canali di segnalazione esterni, come quelli gestiti dagli organismi di regolamentazione, devono affrontare ulteriori sfide per bilanciare la

trasparenza con la protezione dei dati. Canali di comunicazione sicuri sono essenziali per proteggere l'integrità delle segnalazioni e impedire l'accesso non autorizzato alle informazioni sensibili. Le organizzazioni che gestiscono canali esterni dovrebbero **stabilire politiche chiare che delineino il trattamento dei dati personali,** comprese le procedure per **verificare l'autenticità** delle segnalazioni e **proteggere l'identità** dellə segnalanti.

La trasparenza e la piena informazione (cfr. capitolo 1) è fondamentale: chi segnala dovrebbe avere a disposizione anche opzioni di anonimato, oltre alla strada della riservatezza, con meccanismi per una comunicazione sicura di seguito alla segnalazione. La protezione fornita allə segnalanti rientra nelle finalità legittime previste dal GDPR, per cui fornire informazioni a una persona oggetto di una segnalazione mentre l'indagine è in corso, può danneggiare l'indagine stessa portando all'identificazione di chi ha segnalato. L'uso di sistemi sicuri e verificabili può garantire la responsabilità e il rispetto dei requisiti di protezione dei dati. Gli organismi di regolamentazione dovrebbero anche prendere in considerazione l'implementazione di controlli di accesso a più livelli e solidi protocolli di crittografia per proteggere le informazioni sensibili.

Gli *audit* periodici di terze parti di questi sistemi forniscono un ulteriore livello di garanzia del rispetto dei principi di protezione dei dati. Per garantire la fiducia del pubblico, i canali di segnalazione esterna devono anche porre l'accento sull'equità e l'imparzialità. Tali misure dimostrano un impegno a favore sia della protezione dei dati che dell'*accountability*, rafforzando la fiducia nei sistemi di segnalazione esterna.

3.9.1 Buone pratiche dall'Italia

Per ottemperare a tutti i requisiti del GDPR sopra citati, in **Italia**, il D.Lgs. 24/2023 prevede che le segnalazioni non possano essere utilizzate oltre a quanto necessario per darvi un seguito adeguato. **L'identità della persona segnalante e qualsiasi altra informazione da cui tale identità possa essere dedotta, direttamente o indirettamente, non possono essere rivelate, senza il loro esplicito consenso,** a soggetti diversi da quelli competenti a ricevere le segnalazioni o a darvi seguito, espressamente autorizzati a trattare tali dati ai sensi del GDPR Artt. 29 e 32, Par. 4[59]. Si prevede, inoltre, che i dati personali manifestamente non utili per l'elaborazione di una specifica segnalazione non siano raccolti o, se raccolti accidentalmente, siano cancellati immediatamente (Art. 13.2).

Le segnalazioni interne ed esterne e la relativa documentazione sono **conservate per il tempo necessario** all'elaborazione della segnalazione **e comunque non oltre cinque anni** dalla data di comunicazione dell'esito definitivo della procedura di segnalazione, secondo una specifica disposizione della normativa italiana in materia di protezione dei dati

[59] *Regolamento generale sulla protezione dei dati:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

personali (Art. 2-undecies del D.Lgs. 196/2003, introdotto con il D.Lgs. 101/2018).

3.9.2 Mitigazione dei rischi reputazionali

Anche i canali di segnalazione esterni devono affrontare maggiori rischi reputazionali quando le informazioni sensibili diventano pubbliche, come sottolineato da alcuni soggetti intervistati italiani. **Le divulgazioni dei dipendenti tramite i *social media***, per esempio, **possono danneggiare in modo significativo la reputazione** di un'azienda o di un'amministrazione pubblica. L'attuazione di politiche rigorose in materia di divulgazione al pubblico e la promozione di canali di segnalazione esterni sicuri possono mitigare questi rischi. L'Art. 11-ter del Codice di Autodisciplina sottolinea questo tema, dimostrando la necessità di un allineamento tra le legislazioni nazionali e le disposizioni della Direttiva. Per contrastare i rischi reputazionali nel rispetto dei principi della Direttiva, le organizzazioni possono offrire molteplici vie di segnalazione sicure e ufficiali, tra cui linee telefoniche riservate e piattaforme *online* crittografate. Questi canali possono evitare che lə segnalanti ricorrano ai *social media*, mantenendo così la riservatezza e limitando i danni alla reputazione.

3.9.3 Competenza e formazione

Il *feedback* ricevuto delle interviste spagnole evidenzia **l'importanza fondamentale delle competenze in materia di protezione dei dati**. Le organizzazioni dovrebbero garantire che il personale che gestisce i canali di segnalazione esterni sia adeguatamente formato e possieda una conoscenza approfondita dei requisiti del GDPR. *Workshop* e programmi di certificazione regolari per lə Responsabili della Protezione dei Dati **(RPD, o internazionalmente DPO, *Data Protection Officer***) e altro personale pertinente possono rafforzare la *compliance* e promuovere una cultura che metta la *privacy* al primo posto. Attuando queste misure, i canali di segnalazione esterna possono raggiungere il duplice obiettivo di promuovere la trasparenza e salvaguardare i diritti di tutte le parti coinvolte, promuovere la fiducia e il rispetto della legge.

3.10. MISURE TECNICHE E ORGANIZZATIVE

L'attuazione di solide misure tecniche e organizzative è essenziale per garantire la conformità al GDPR[60] e salvaguardare i dati personali. La crittografia e la pseudonimizzazione sono tecniche ampiamente riconosciute che migliorano la sicurezza dei dati rendendoli incomprensibili a parti non autorizzate. I controlli degli accessi basati sui ruoli limitano l'accesso ai dati al personale autorizzato, riducendo il rischio di divulgazioni non autorizzate.

[60] *Regolamento generale sulla protezione dei dati (Art. 24):* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Le organizzazioni devono sviluppare e implementare politiche complete di protezione dei dati che delineino ruoli, responsabilità e procedure per la gestione dei dati personali. Programmi regolari di formazione e sensibilizzazione per i dipendenti assicurano che tutte le parti interessate comprendano i loro obblighi ai sensi del GDPR e dei quadri di protezione dellə segnalanti. *Audit* periodici e valutazioni dei rischi aiutano a identificare le vulnerabilità e a garantire che le misure di sicurezza rimangano efficaci e aggiornate.

I piani di risposta agli incidenti sono importanti per affrontare le violazioni dei dati e ridurne al minimo l'impatto. Le organizzazioni devono stabilire protocolli chiari per rilevare, segnalare e mitigare le violazioni, nonché informare le persone e le autorità interessate, ove necessario.

3.11. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA NELLA DIVULGAZIONE AL PUBBLICO

Il terzo canale della divulgazione pubblica presenta sfide uniche nel bilanciare la protezione dei dati con la necessità di trasparenza e *accountability*. Il modo in cui le organizzazioni rispettano i loro obblighi in materia di protezione di chi segnala in questi casi è essenziale. **La divulgazione pubblica,** infatti, rappresenta la forma più sensibile di *whistleblowing*, dove il **potenziale di danno reputazionale e le implicazioni legali sono più elevate**. Ai sensi della Direttiva (e per come ben raccontato in **capitolo 1**), la divulgazione al pubblico è considerata l'ultima risorsa, consentita solo quando i canali di segnalazione interni ed esterni sono stati esauriti o sono ritenuti inefficaci. Prima di divulgare informazioni al pubblico, le organizzazioni (nel ruolo di canali di segnalazione esterni o interni) devono valutare attentamente se la divulgazione è in linea con i principi del GDPR e serve l'interesse pubblico. Il consenso esplicito dovrebbe essere ottenuto ogniqualvolta possibile, in particolare quando si tratta di dati personali sensibili.

Cp. 1 >

3.11.1 Il ruolo della protezione dei dati nelle divulgazioni pubbliche

Nel contesto delle divulgazioni pubbliche, **sia le piattaforme che supportano la divulgazione sia chi segnala** devono navigare con attenzione sulla **linea sottile tra tutela dell'interesse collettivo, trasparenza e danno reputazionale**. I protocolli di redazione svolgono un ruolo fondamentale nella protezione della *privacy* durante le divulgazioni pubbliche. Le piattaforme che supportano la divulgazione devono rimuovere o oscurare i dati personali che non sono essenziali per raggiungere lo scopo della divulgazione. Ciò garantisce il rispetto del principio della minimizzazione dei dati, salvaguardando al contempo i diritti delle persone. Il già citato *software GlobaLeaks* dall'Italia esemplifica come la tecnologia possa supportare anche le divulgazioni pubbliche. Anonimizzando e crittografando le comunicazioni, tali piattaforme

consentono a chi segnala di condividere le informazioni in modo sicuro, riducendo i rischi associati alle divulgazioni pubbliche non regolamentate. L'integrazione di tale tecnologia nei quadri di divulgazione al pubblico può garantire la conformità alla Direttiva, mantenendo al contempo la fiducia del soggetto segnalante.

In **Italia**, come registrato anche nelle interviste fatte, **è emersa la preoccupazione per il potenziale uso improprio delle divulgazioni pubbliche** tramite i *social media*, possibilità prevista dalla Direttiva. Quando lə segnalanti aggirano i meccanismi formali di segnalazione e divulgano informazioni sensibili su piattaforme aperte, non solo mettono ovviamente a repentaglio la riservatezza (facendo automaticamente saltare la prima forma di tutela, ossia la non emersione del proprio nome), ma possono generare anche rischi significativi per la reputazione aziendale o istituzionale.

Cp. 1 >

Le organizzazioni, a riguardo (cfr. capitolo 1) sono tenute a informare lə dipendenti sui limiti legali delle divulgazioni pubbliche. L'Art. 11-ter del Codice di Condotta, per esempio, affronta il tema dell'uso sconsiderato dei *social network* e sottolinea l'importanza di aderire a meccanismi di segnalazione strutturati. L'integrazione di queste misure con canali interni ed esterni accessibili e solidi può ridurre la probabilità che lə segnalanti ricorrano a piattaforme pubbliche. Tuttavia, **in Italia permane un disallineamento tra le disposizioni del Codice di Condotta e il D.Lgs. 24/2023 in materia di *whistleblowing*.** Quest'ultimo riconosce esplicitamente la possibilità di divulgazione al pubblico a determinate condizioni, una sfumatura che non trova adeguata riscontro nel Codice. Allo stesso tempo, il mancato allineamento tra il Codice di Autodisciplina e l'attuale quadro normativo crea confusione riguardo al destinatario delle segnalazioni interne, in quanto individua ancora in modo errato il superiore gerarchico al posto del Responsabile della Prevenzione della Corruzione e della Trasparenza. Tale situazione richiederebbe un intervento legislativo tempestivo.

3.11.2 Come migliorare la sicurezza nelle divulgazioni pubbliche?

In questa guida, sosteniamo l'idea che per allineare la divulgazione pubblica con i principi di protezione dei dati, **le piattaforme che supportano e le autorità di vigilanza dovrebbero elaborare orientamenti e misure di protezione chiari,** come per esempio:

A. Stabilire protocolli per verificare l'accuratezza delle informazioni riportate.
B. Documentare tutte le azioni intraprese in risposta alla divulgazione.
C. Garantire una comunicazione trasparente su questi processi.

La prospettiva spagnola e bulgara, per come raccolto dalle interviste, sottolinea l'importanza di limitare l'accesso al terzo canale al personale

essenziale. In **Italia**, tale interpretazione è vista come eccessivamente restrittiva, rischiando di compromettere il senso stesso della divulgazione pubblica.

3.12. PROTEZIONE DEI DATI E CENTRI D'INFORMAZIONE ORGANIZZATI DALLA SOCIETÀ CIVILE: UNA QUESTIONE APERTA

Cp. 2>

Cp. 4>

L'Art. 20 della Direttiva riconosce il ruolo dei **centri di informazione** (cfr. capitolo 2) come **servizi di supporto che (anche) la società civile può organizzare** e mettere a disposizione per aiutare lə potenziali segnalanti ad affrontare dilemmi etici e dubbi sul funzionamento del sistema. La legge stabilisce che questo ruolo possa parimenti essere svolto da **istituzioni dedicate**. Per poter adempiere a tale compito (cfr. capitolo 4), tali centri di informazione entrano necessariamente in contatto, gestiscono e (in forme minime) conservano dati personali, nonché altre informazioni sensibili. A questo proposito, la disposizione iniziale n. 89 della Direttiva stabilisce che **i centri di informazione** "**sono tenuti a mantenere la riservatezza delle informazioni ricevute**".

Tuttavia, la Direttiva non fornisce ulteriori dettagli sulle modalità per adempiere a tale obbligo, sull'opportunità di equiparare tali centri agli enti che ricevono segnalazioni tramite canali interni o esterni, o sull'applicazione di condizioni speciali. **La Direttiva rimane vaga su questo punto**. Questa lacuna non è stata sufficientemente affrontata nelle normative dei vari Paesi, in particolare considerando che, salvo rare eccezioni, tali servizi di supporto non sono ancora ampiamente praticati in tutta Europa.

In **Italia**, dove tali centri civici di supporto esistono, funzionano e sono formalmente riconosciuti, si riscontra, allo stato della scrittura di queste pagine, l'assenza di linee guida specifiche sulle pratiche di trattamento dei dati. **Vi è quindi il rischio che ai servizi di supporto possa essere impedito di elaborare i dati**, limitando così le loro funzioni (e potenzialmente compromettendo la loro capacità di operare del tutto), limitando al contempo l'accesso dei potenziali segnalanti all'assistenza.

Nella presente guida, **suggeriamo come le normative nazionali**, o gli orientamenti forniti dalle autorità competenti per il *whistleblowing*, **dovrebbero mirare a colmare questa lacuna stabilendo protocolli chiari** per il trattamento dei dati che consentano allə segnalanti di ricevere supporto, imponendo nel contempo ai centri di informazione di implementare sistemi di crittografia rafforzati per la ricezione, l'archiviazione (per un periodo limitato) e la condivisione dei dati tra lə operatori, garantendo al meglio la protezione e la riservatezza delle informazioni del segnalante.

Inoltre, suggeriamo che, così come previsto nel Considerando 74 della Direttiva (che impone ai membri del personale delle autorità competenti responsabili del trattamento delle segnalazioni di ricevere una **formazione**

professionale anche sulle norme in materia di protezione dei dati) anche chi, appartenente al terzo settore, opera un servizio civico di supporto debba essere adeguatamente formato. È essenziale poi che esista un confronto attivo tra enti civici anche sui temi della gestione della *privacy*, con l'emersione delle migliori pratiche e delle lezioni apprese, includendo momenti di **scambio e confronto** con le **autorità competenti sul tema**, anche agendo in sinergia con altre reti che pure si occupano di accompagnamento e di vittime (in **Italia**, rete Dafne).

FOCUS GOVERNO APERTO

Solide strategie di protezione dei dati sono fondamentali per una varietà di *stakeholder*, come lə segnalanti, i gestori dei canali di segnalazione, i soggetti che offrono sostegno a potenziali segnalanti come le organizzazioni della società civile e i soggetti che hanno un ruolo come canale di divulgazione pubblica, come giornalistə e gli organi di stampa. Tali strategie dovrebbero includere meccanismi sicuri per la gestione delle informazioni sensibili al fine di salvaguardare l'identità e gli interessi dellə segnalanti. **La collaborazione intersettoriale** con il coinvolgimento delle autorità nazionali di regolamentazione, dei responsabili della protezione dei dati e dei responsabili politici **può essere decisiva** per lo sviluppo di soluzioni innovative di protezione dei dati su misura per i diversi scenari di *whistleblowing*, in particolare **per affrontare le complessità delle divulgazioni pubbliche.** Gli sforzi congiunti possono armonizzare le legislazioni nazionali con le disposizioni della Direttiva, elaborando orientamenti chiari sull'uso etico dei dati per aiutare tutte le parti interessate a mantenere la trasparenza nel rispetto della *privacy*.

Un tema sempre più critico da affrontare in un quadro di governo aperto è il **trattamento dei dati sensibili e personali da parte di centri di informazione** - sia civici che istituzionali - riconosciuti dalla Direttiva. La Direttiva stessa (nelle disposizioni iniziali 89 e 90) impone a tali soggetti di garantire un trattamento efficace dei dati, anche se non fornisce ulteriori specifiche.

I servizi di supporto e consulenza, nel loro ruolo di indirizzo dellə potenziali segnalanti , entrano inevitabilmente in contatto con dati sensibili. Il loro scopo non è semplicemente quello di fornire informazioni generiche e decontestualizzate, ma piuttosto di aiutare le persone a navigare nei canali di segnalazione appropriati in modo significativo. Un approccio puramente neutro e distaccato non riuscirebbe a soddisfare le esigenze dei potenziali segnalanti.

La questione dovrebbe essere discussa apertamente in un contesto di governo aperto, attraverso lo sviluppo di linee guida chiare, organizzando discussioni congiunte che coinvolgano le autorità di protezione dei dati, i rappresentanti dei centri di informazione (sia civici che istituzionali) e gli organismi di regolamentazione del *whistleblowing*.

L'obiettivo dovrebbe essere quello di trovare il giusto equilibrio tra due esigenze fondamentali: garantire che lə potenziali segnalanti ricevano un'assistenza significativa (che potrebbe richiedere un alto livello di trattamento dei dati da parte dei servizi di supporto) e salvaguardare al contempo i loro dati personali.

Per esempio, le discussioni dovrebbero stabilire:

A. **Criteri di conservazione chiari**, incluso un periodo massimo di archiviazione per i dati sensibili.
B. **Metodi sicuri e riservati per lo scambio di dati** tra potenziali segnalanti e servizi di supporto.
C. **Protocolli di comunicazione** definiti tra i consulenti all'interno dello stesso servizio.

Un'interpretazione restrittiva che dia priorità alla *privacy* sopra ogni altra cosa potrebbe involontariamente minare gli interessi stessi di potenziali segnalanti, limitando la loro capacità di cercare un'assistenza efficace.

3.13 RACCOMANDAZIONI

La Fondazione *Konrad Adenauer* (KAF), nel corso del suo lavoro su vari progetti e *policy*, sottolinea che un quadro giuridico completo (simile al GDPR[61]) è essenziale per promuovere la trasparenza e salvaguardare i diritti individuali, definendo chiaramente l'ambito e i confini delle attività di *whistleblowing*. KAF promuove l'adozione di meccanismi che sostengano il principio di proporzionalità nella gestione dei dati, bilanciando la necessità di indagare su una cattiva condotta segnalata con il diritto alla *privacy* di tutti gli individui coinvolti. Sottolineano inoltre l'importanza delle campagne di sensibilizzazione pubblica per educare lə cittadinə e le organizzazioni sui loro diritti e responsabilità nell'ambito del *whistleblowing*. Sono stati elencati alcuni consigli pratici per l'attuazione delle politiche di protezione dei dati[62]:

1. ISTITUIRE ORGANI DI CONTROLLO INDIPENDENTI

Richiamarsi ai principi alla base del GDPR aiuta a evitare una lettura meramente formale della *privacy*, riducendola a un adempimento anziché riconoscerla come garanzia attiva.

2. AUTORITÀ DEGLI ORGANI INDIPENDENTI

Dovrebbero essere istituiti organismi di vigilanza indipendenti per monitorare l'attuazione dei meccanismi di *whistleblowing*, come definito dal quadro giuridico nazionale applicabile.

3. IMPORTANZA DEI PROGRAMMI DI FORMAZIONE

Tali organismi dovrebbero avere l'autorità di esaminare le segnalazioni, esaminare le pratiche di protezione dei dati e garantire il rispetto delle norme giuridiche, quando si tratta di autorità indipendenti che ricevono segnalazioni attraverso un canale esterno (o il loro canale interno).

4. GESTIONE DELLE SEGNALAZIONI SENSIBILI E RISERVATEZZA

I programmi di formazione per lə dipendenti del settore pubblico e privato sono fondamentali per creare consapevolezza sui protocolli di *whistleblowing* e sui principi di protezione dei dati.

5. BUONE PRATICHE PER RAFFORZARE LA CONFORMITÀ

Lə dipendenti devono essere in grado di riconoscere l'importanza della riservatezza, gestire in modo sicuro le segnalazioni sensibili ed evitare

---

[61] *Si veda:* https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_47778_2.pdf/c2a538a2-ed3d-1aa7-b2ae-2736329c8a66?version=1.0&t=1539649646584

[62] *Trasparenza e responsabilità:* https://www.kas.de/en/web/rspno/veranstaltungsberichte/detail/-/content/transparenz-und-rechenschaftspflicht

divulgazioni non autorizzate.

Nel complesso, ecco alcune buone pratiche che le organizzazioni possono seguire per rafforzare la propria conformità e promuovere la fiducia:

5.1 SVILUPPO DI POLITICHE DETTAGLIATE SULLA DENUNCIA DELLE SEGNALAZIONI

Le organizzazioni dovrebbero sviluppare **politiche dettagliate che delineino lo scopo, l'ambito e le procedure** dei loro sistemi di *whistleblowing*. Queste politiche devono soddisfare i requisiti di protezione dei dati, tra cui la raccolta, l'archiviazione, l'elaborazione e la conservazione dei dati. Rendendo queste politiche accessibili a tutte le parti interessate, le organizzazioni dimostrano trasparenza e *accountability*.

5.2 NOMINA DI UN RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)ВАНЕ НА ОЦЕНКИ НА РИСКА ПРЕДИ ПУБЛИЧНО ОПОВЕСТЯВАНЕ

La nomina di unə responsabile della protezione dei dati (RPD, o internazionalmente DPO, *Data Protection Officer*) qualificato è fondamentale per garantire la conformità continua al GDPR e alla Direttiva sul *whistleblowing*. Lə RPD possono fornire indicazioni sulla gestione dei dati personali, condurre *audit* e fungere da punto di contatto per i soggetti interessati e le autorità di vigilanza.

5.3 ADATTARE I PROGRAMMI DI FORMAZIONE ALLE PARTI INTERESSATE

I programmi di formazione dovrebbero essere adattati alle esigenze dei diversi gruppi di *stakeholder*, compresi lə dipendenti, lə dirigenti e i fornitori esterni di servizi. Questi programmi dovrebbero sottolineare l'importanza della riservatezza, della minimizzazione dei dati e dei diritti dei soggetti interessati. La formazione basata su scenari può aiutare lə dipendenti a capire come gestire efficacemente i casi di *whistleblowing* sensibili.

5.4 IMPLEMENTARE CANALI DI SEGNALAZIONE SICURI

Le organizzazioni dovrebbero implementare **canali di segnalazione sicuri e di facile utilizzo** che consentano allə segnalanti di inviare informazioni in modo riservato. L'autenticazione a più fattori e i protocolli di comunicazione crittografati possono migliorare la sicurezza di questi sistemi. Inoltre, le organizzazioni dovrebbero testare regolarmente questi sistemi per identificare e affrontare le vulnerabilità.

5.5 MONITORAGGIO E AUDIT PERIODICI

Il monitoraggio e l'*audit* periodici dei sistemi di *whistleblowing* contribuiscono a garantire la conformità ai requisiti di protezione dei dati. Le organizzazioni dovrebbero tenere registri dettagliati delle attività di trattamento dei dati, comprese le giustificazioni per la raccolta e la conservazione dei dati. Gli *audit* possono identificare le lacune nella conformità e fornire opportunità di miglioramento continuo.

5.6 COLLABORAZIONE CON GLI ORGANI DI REGOLAMENTAZIONE

L'interazione con le autorità nazionali per la protezione dei dati e altri organismi di regolamentazione può aiutare le organizzazioni a rimanere informate sui cambiamenti della legislazione e delle migliori pratiche. La collaborazione facilita anche la risoluzione di casi complessi, come quelli che riguardano trasferimenti transfrontalieri di dati o conflitti tra normative nazionali e dell'UE.

5.7 UTILIZZO DI TECNOLOGIE INNOVATIVE

Tecnologie innovative, come l'intelligenza artificiale e l'apprendimento automatico, potrebbero migliorare l'efficienza e la sicurezza dei sistemi di *whistleblowing*. Per esempio, gli strumenti basati sull'intelligenza artificiale possono rilevare modelli di comportamenti illeciti, identificare le violazioni dei dati e supportare i processi di anonimizzazione. Tuttavia, le organizzazioni devono garantire che queste tecnologie siano conformi al GDPR e ad altre normative applicabili.

5.8 DEFINIZIONE DI PARAMETRI DI EFFICACIA

Le organizzazioni dovrebbero **stabilire metriche per valutare l'efficacia dei loro sistemi di *whistleblowing***, tra cui il tasso di risoluzione dei casi segnalati, i livelli di soddisfazione dellə segnalanti e la conformità generale dell'organizzazione agli *standard* di protezione dei dati. La rendicontazione periodica di queste statistiche può creare fiducia tra le parti interessate ed evidenziare le aree di miglioramento (cfr. **capitolo 5**).

Cp. 5>

5.9 PROMUOVERE IL MIGLIORAMENTO CONTINUO

La protezione dei dati è un processo continuo che richiede alle organizzazioni di **adattarsi ai mutevoli scenari legali, tecnologici e sociali.** Promuovendo una cultura del miglioramento continuo, le organizzazioni possono garantire che i loro sistemi di *whistleblowing* rimangano efficaci, sicuri e conformi agli *standard* in evoluzione. Incorporando queste strategie/buone pratiche, le organizzazioni e i governi nazionali possono istituire meccanismi di *whistleblowing* che siano conformi alla legge e praticamente efficaci. Questi sistemi non solo incoraggiano le persone a segnalare con sicurezza i comportamenti scorretti, ma rafforzano anche la *governance* generale, migliorano la fiducia del pubblico e contribuiscono a una cultura dell'integrità.

5.10 BILANCIARE L'INTERESSE PUBBLICO CON IL DIRITTO ALLA PRIVACY

Per bilanciare l'interesse pubblico con i diritti alla *privacy* è necessaria una valutazione della proporzionalità, che tenga conto di fattori quali la gravità del problema segnalato, il potenziale impatto della divulgazione e la disponibilità di soluzioni alternative. Le organizzazioni devono documentare i loro processi decisionali per dimostrare la responsabilità e la conformità ai requisiti normativi quali registri interni, regole e procedure, codici di condotta e codici etici.

5.11 DARE PRIORITÀ ALLA RISERVATEZZA DEI SEGNALANTI NELLE DIVULGAZIONI PUBBLICHE

I meccanismi di divulgazione pubblica devono dare priorità al mantenimento della riservatezza dellə segnalanti, a meno che non venga fornito il consenso esplicito. Le organizzazioni dovrebbero stabilire procedure chiare e accessibili per consentire allə segnalanti di esprimere le loro preferenze in merito alla divulgazione e garantire che tali preferenze siano rispettate.

5.12 EFFETTUARE VALUTAZIONI DEL RISCHIO PRIMA DELLA DIVULGAZIONE PUBBLICA

Per quanto riguarda la divulgazione al pubblico, dovrebbero essere attuati solidi quadri di valutazione del rischio per **valutare le potenziali conseguenze della divulgazione di informazioni.** Ciò include la valutazione della probabilità di danno per lə segnalanti, le persone coinvolte o il pubblico. Quando possibile, prima della divulgazione dovrebbero essere applicate tecniche di anonimizzazione e pseudonimizzazione ai dati.

5.13 UTILIZZO DI STRUMENTI DI REVISIONE AUTOMATICA

L'uso di soluzioni tecnologiche, come gli **strumenti di oscuramento automatizzati, può semplificare la preparazione dei dati per la divulgazione pubblica.** Questi strumenti sono in grado di rilevare e mascherare le informazioni personali sensibili in modo coerente ed efficiente, riducendo al minimo il rischio di errore umano.

5.14 DEFINIRE I CRITERI PER LA DIVULGAZIONE PUBBLICA

Le organizzazioni devono inoltre **stabilire criteri chiari per determinare quando la divulgazione al pubblico è appropriata.** I fattori da considerare includono l'urgenza del problema, la disponibilità di meccanismi di segnalazione interni o esterni e i potenziali benefici e rischi della divulgazione.

5.15 FORMARE IL PERSONALE COINVOLTO NELLE DIVULGAZIONI PUBBLICHE

Infine, sono essenziali i **programmi di istruzione e formazione per il personale coinvolto nei processi di divulgazione al pubblico.** Tali programmi dovrebbero riguardare gli aspetti giuridici ed etici della protezione dei dati, l'importanza di conciliare la *privacy* con la trasparenza e le competenze tecniche necessarie per gestire le informazioni sensibili.

Protezione e sostegno dellə segnalanti

Capitolo 4

Open the whistle

PROTEZIONE E SOSTEGNO DELLƎ SEGNALANTI

Capitolo 4

4. 1 PROTEZIONE PREVISTA DALLA DIRETTIVA (UE) 2019/1937

Un quarto ambito determinante che abbiamo voluto trattare in questa guida è quello delle forme di protezione e **sostegno di tutte le figure che, a diverso titolo, ruotano attorno all'istituto del *whistleblowing*.**

La Direttiva prevede anzitutto **una protezione completa alle persone che segnalano** illeciti, garantendo al tempo stesso anche **forme di tutela da ritorsioni post-segnalazione** e a chi, a diverso titolo, è coinvoltə nella segnalazione. L'innovazione sta nell'estendere la protezione, oltre allə solə dipendenti (per come era in **Italia** fino a prima della norma di recepimento), a:

A. Lə già citatə dipendenti pubblicə, ma anche lə lavoratorə autonomə come liberə professionistə e appaltatorə indipendenti (TFUE Art. 49).
B. Azionistə e consiglierіə non esecutivi.
C. Volontari e tirocinanti, retribuitə o non retribuitə.
D. Ex lavoratorə.
E. Facilitatorə, ovvero quelle persone che, condividendone il luogo di lavoro, assistono lə segnalanti in modo confidenziale nel processo di segnalazione.
F. Terze parti che potrebbero subire ritorsioni a causa del loro legame con lə segnalante, inclusi familiari, colleghə e persino persone giuridiche legate alla persona segnalante.
G. Centri d'informazione civici, ossia servizi di supporto e accompagnamento messi a disposizione da organizzazioni della società civile, i quali potrebbero subire pressioni proprio in virtù del proprio ruolo.

La protezione rimane valida indipendentemente dal canale scelto, purché la divulgazione sia conforme alle disposizioni della Direttiva, quindi delle normative nazionali. Se i meccanismi interni o esterni si rivelano inefficaci o se vi è una minaccia imminente per l'interesse pubblico, lə segnalanti possono rendere pubbliche le informazioni sulle violazioni senza perdere la loro base giuridica per la protezione.

Per come riportato in numerose interviste in tutti e tre i Paesi coinvolti, accade che i **diversi *stakeholder* percepiscono i canali interni come meno sicuri di quelli esterni, in particolare quando le segnalazioni sono divergenti con gli interessi di un'organizzazione**. Moltə temono ritorsioni e questa preoccupazione si estende al personale addetto alla ricezione e alla gestione delle segnalazioni, che (riportano intervistatə italianə sulla

situazione della Penisola) spesso non è indipendente dalla propria organizzazione e non gode delle necessarie tutele che consentirebbero loro di perseguire efficacemente le segnalazioni.

Un aspetto che intendiamo attenzionare riguarda il fatto che la protezione dellə segnalanti non si applica direttamente alla stampa qualora divulghi notizie ottenute per tramite di segnalanti; in tal caso vigono le leggi nazionali che stabiliscono tutele specifiche per la libertà di espressione e d'informazione (Art. 15, Par. 2). Pertanto, è bene chiarire espressamente che allo stato dell'arte **lə giornalistə sono esclusə dalle tutele della Direttiva**, sebbene il tema sia ampiamente discusso. In **Bulgaria**, per esempio, la discussione riguarda come integrare il concetto di SLAPP (acronimo inglese che in italiano suona come "Cause legali strategiche contro la partecipazione pubblica") e le normative a tutela delle segnalanti, per proteggere il mondo della stampa da azioni legali. Le cause SLAPP vengono usate da potenti interessi (come aziende o politici) per bloccare o rallentare il lavoro giornalistico, spesso con accuse infondate e azioni legali molto costose, scoraggiando dal proseguire in inchieste su temi delicati, come la corruzione o altre questioni di interesse pubblico. L'introduzione di leggi che proteggano sia segnalanti che giornalistə in questi contesti, "armonizzando le normative (sia come diritto dell'UE che nazionale), potrebbe rafforzare la libertà di stampa e incentivare una maggiore trasparenza".

4.1.2 Cosa deve fare lə segnalante per qualificarsi per beneficiare della protezione?

Ciò che è bene specificare, prima ancora di parlare delle tutele, è che, al fine di qualificarsi per la protezione (ai sensi della Direttiva quindi di ogni normativa nazionale di recepimento), lə segnalanti devono soddisfare **due condizioni specifiche: agire nel pubblico interesse ed effettuare la segnalazione attraverso canali appropriati.** Fermo quanto detto, è sufficiente la ragionevole convinzione che le informazioni divulgate siano vere. La Direttiva non prende in considerazione, né consente, valutazioni soggettive dei motivi che spingono unə segnalante a riportare una violazione. Pertanto, ed è bene specificarlo: la "**buona fede" (intesa come intima intenzione del segnalante) non è un fattore rilevante**. Ciò che conta è che il soggetto segnalante ritenga ragionevolmente che un reato sia stato commesso o possa essere commesso.

Cosa costituisce una "convinzione fondata"?

La **fondatezza si basa su elementi oggettivi e concreti**, come (una sorta di) prove o comunque indicazioni verificabili quanto più possibile dall'esterno, che inducono la persona segnalante a credere che i fatti presentati siano veri. Ciò significa che, anche se le informazioni segnalate si dovessero rivelare in seguito errate, la persona segnalante rimane comunque protetta in quanto aveva motivi legittimi per considerare tali informazioni accurate al momento della segnalazione. Questa salvaguardia è fondamentale per incoraggiare le persone a farsi avanti senza timore di essere sanzionate per errori non intenzionali.

Diversamente, come già detto, **il motivo personale e soggettivo della segnalazione è irrilevante** per la protezione di chi la invia e ai fini della stessa. Questo principio è ribadito nel Considerando 32 della Direttiva e ribadito nella risoluzione 10/8 dell'UNCAC "Protezione delle persone segnalanti" (Par. 14).

Dopo il 2019, pertanto, **grazie alla Direttiva c'è stato un passaggio definitivo dalla valutazione delle motivazioni personali di unə segnalante alla valutazione dei fatti oggettivi della segnalazione stessa**. In estrema sintesi: ciò che conta è che le segnalazioni siano coerenti con la tutela dell'interesse pubblico, dell'integrità della pubblica amministrazione o dell'ente privato: i motivi che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della loro tutela. Tuttavia, la Convenzione europea dei diritti dell'uomo (CEDU) continua a includere il principio della "buona fede" come requisito di protezione, il che crea un chiaro conflitto con la Direttiva, che in alcuni casi si ripercuote in alcune normative nazionali (non è tuttavia il caso dell'**Italia**).

Il principio di ragionevolezza svolge poi, di per sé, anche un ruolo cruciale nella prevenzione di segnalazioni dolose (ossia affermazioni manifestamente false), che potrebbero danneggiare ingiustamente persone od organizzazioni.

Protezione nelle segnalazioni anonime

La Direttiva riconosce che le segnalazioni anonime possono contribuire a creare fiducia nei sistemi di *whistleblowing*. Con segnalazioni anonime, si intendono quelle in cui chi segnala sceglie di non fornire la propria identità, la quale rimane sconosciuta anche a chi riceve la segnalazione e a chi gestisce il canale. Come già più volte detto, l'anonimato non coincide con la "riservatezza", dove l'identità del soggetto segnalante è nota ma protetta. Lə segnalanti che scelgono di effettuare una segnalazione anonima e successivamente rivelano la propria identità rimangono idoneə alla protezione in caso di ritorsioni (Art.6.3). Tuttavia, il trattamento delle segnalazioni anonime varia tra i tre Paesi coinvolti in questo progetto e, più in generale, in Europa.

La normativa italiana, per esempio, non incoraggiandole, prevede una gestione differente delle segnalazioni anonime. ANAC, infatti, tratta come segnalazioni ordinarie, fino all'invocazione della tutela, le segnalazioni anonime che arrivano tramite canale esterno.

Resta salvo il riconoscimento della tutela allə segnalanti anonimi che subiscono ritorsioni. Se unə segnalante anonimə subisce successivamente ritorsioni, ha diritto alle stesse tutele dellə segnalanti non anonimə (D.Lgs. 24/2023 Art. 6). **Una differenza fondamentale** per quanto riguarda la segnalazione anonima è che l'accesso alla segnalazione è consentito alle condizioni e alle limitazioni specifiche stabilite dalla legge italiana. Ciò in quanto **le denunce anonime sono assimilate alle denunce ordinarie** ai sensi delle disposizioni di legge generali:

A. Accesso documentale e difensivo (Legge 241/1990 Artt. 22 e ss.).
B. Accesso civico (Artt. 5 e ss. del D.Lgs. n. 33 del 2013).

La Bulgaria non regolamenta formalmente la segnalazione anonima di irregolarità. Tuttavia, le persone che hanno presentato segnalazioni anonime o divulgato pubblicamente informazioni sulle violazioni e che sono successivamente identificate e oggetto di ritorsioni, hanno diritto alla protezione (Legge bulgara Art. 10).

La Spagna consente la segnalazione anonima e impone la protezione dellə segnalanti che vengono successivamente identificatə e sottopostə a ritorsioni (Art. 7, Par. 3 per il canale interno, Art. 17 per il canale esterno, Legge 2/2023). Ai sensi del diritto spagnolo, la violazione delle garanzie di riservatezza e anonimato costituisce una violazione molto grave nell'ambito del regime sanzionatorio. È vietata qualsiasi azione od omissione volta a rivelare l'identità di unə segnalante che ha optato per l'anonimato, anche se la divulgazione effettiva non avviene.

4.2 MISURE DI SOSTEGNO DEI SOGGETTI OBBLIGATI

Chiarito il quadro che abilita all'ottenimento delle misure, veniamo finalmente a esse. La propedeutica misura di sostegno (Direttiva, Art. 20) consiste nel **poter accedere a informazioni e consulenze complete e indipendenti, facilmente accessibili al pubblico e gratuite** (cfr. capitolo 1). Ciò include orientamenti sulle procedure e i mezzi di ricorso disponibili, sulla protezione contro le ritorsioni, sui diritti della persona segnalata.

Cp. 1 ›

4.2.1 Il ruolo delle autorità

Il Considerando 90 della Direttiva prevede che le **autorità competenti forniscano allə segnalanti il sostegno necessario per accedere efficacemente alla protezione.** In particolare, dovrebbero fornire prove o altra documentazione che confermi ad altre autorità o tribunali che la segnalazione esterna ha avuto luogo e garantire che lə segnalanti comprendano i loro diritti e le risorse disponibili. In dettaglio, esse:

A. Devono sostenere attivamente lə segnalanti che subiscono ritorsioni, fungendo da imprescindibile punto di contatto.
B. Devono pertanto attivare specifiche procedure che permettano allə segnalanti in ritorsione di segnalare tale loro situazione alle autorità.
C. Valutano se la persona soddisfa i criteri per la protezione e se ha subito misure di ritorsione.
D. Devono garantire che lə segnalanti ricevano un adeguato riconoscimento e assistenza legale.

Specificando ulteriormente, le persone segnalanti dovrebbero ricevere un'assistenza efficace dalle autorità competenti prima di qualsiasi autorità pertinente coinvolta nella loro protezione contro le ritorsioni. Ciò include:

A. **Certificazione**, se prevista dal diritto nazionale, che attesti i requisiti per la protezione.
B. **Patrocinio a spese dello Stato** nei procedimenti penali e civili transfrontalieri, conformemente alla Direttiva (UE) 2019/1937 e alla Direttiva 2008/52/CE del Parlamento europeo e del Consiglio (48).
C. Ove consentito dal diritto nazionale, **patrocinio a spese dello Stato supplementare, consulenza legale o altra assistenza legale** in ulteriori procedimenti.

4.2.2 FORME DI SOSTEGNO PREVISTE DALLA DIRETTIVA (UE) 2019/1937

Supporto psicologico e sociale

Lə potenziali segnalanti che non sono sicurə di come effettuare la segnalazione o se saranno protettə alla fine possono essere scoraggiatə dal segnalare, la Direttiva (Considerando 89 e Art. 20) prevede che **gli Stati membri siano incoraggiati a fornire servizi di consulenza e supporto sociale su misura** per aiutare le persone a far fronte alle sfide emotive e sociali che possono affrontare.

Ciò fa parte delle misure di protezione e include l'offerta di accesso alla consulenza psicologica, nonché a **servizi di consulenza legale e finanziaria** per mitigare le potenziali ripercussioni professionali ed economiche. Inoltre, le reti di supporto, come i **gruppi di pari o i programmi di *mentorship***, possono aiutare lə segnalanti a superare le reazioni sociali e ridurre i sentimenti di isolamento.

Azione legale contro le ritorsioni e inversione dell'onere della prova

Se unə segnalante subisce ritorsioni (si pensi a licenziamento, demansionamento o molestie) ha diritto a **rimedi giuridici effettivi**, tra cui **misure provvisorie** e **risarcimenti completi** (Direttiva, Art. 21). **Esiste quindi il patrocinio a spese dello Stato, con riferimento sia ai procedimenti civili che a quelli penali**. riguardanti casi di protezione dellə segnalanti.

Un aspetto chiave previsto dalla Direttiva, ma che ancora con grande fatica viene accolto nella giurisprudenza dei diversi paesi, riguarda la cosiddetta **inversione dell'onere della prova**: se lə segnalante dimostra di aver effettuato una segnalazione e, in conseguenza temporale di ciò, di aver subito un danno, si presume una ritorsione. Spetta quindi al soggetto segnalato **dimostrare che le misure adottate o le azioni intraprese erano giustificate da motivi indipendenti dalla segnalazione**. L'unico criterio che si può chiedere di dimostrare allə segnalante è quello meramente temporale, ossia della consequenzialità della ritorsione. Se è vero che le corti e i tribunali nazionali dovrebbero assumere un ruolo cruciale nell'applicazione di tali protezioni, garantendo che le persone colpite siano ripristinate al loro *status* precedente e risarcite per i danni subiti, è purtroppo usuale che, persino in sentenze, si preveda diversamente. Su questo occorre ancora una profonda maturazione del sistema e della cultura giuridica, incluso da parte della magistratura.

Alcuni Stati membri hanno attuato anche strumenti economici di sostegno. In Spagna è stato istituito un fondo per l'assistenza legale, sociale e psicologica gratuita per i soggetti segnalanti. Nei Paesi Bassi esiste una struttura analoga. In Francia, lə segnalanti possono ricevere contributi per spese legali e sovvenzioni per far fronte a procedimenti giudiziari, sia per difendersi da azioni intimidatorie, sia per impugnare misure ritorsive.

In Italia, si recepisce l'inversione dell'onere della prova (D.lgs. 24/2023 Art. 20, comma 2): quando unə segnalante dimostra di aver fatto una segnalazione e dichiara di aver subito un pregiudizio, si presume che tale pregiudizio sia conseguenza della segnalazione, salvo prova contraria da parte del datore di lavoro. Purtroppo, però, ci sono sentenze che evidenziano una forte discrepanza tra la normativa vigente e l'applicazione pratica da parte di alcuni tribunali italiani[63].

In questa guida, esprimiamo forte preoccupazione per le volte in cui tale discrepanza va a discapito di chi segnala, la qual cosa genera un'enorme faglia nella fiducia rispetto al sistema.

Nei casi in cui lə segnalante richieda **misure cautelari urgenti** per bloccare ritorsioni già in atto o minacciate, è previsto che debba fornire **elementi che rendano verosimile ("*fumus*") la minaccia o il danno imminente**. Questa regola non contraddice la Direttiva, ma riguarda uno specifico ambito processuale (quello cautelare), in cui è normale che venga richiesta una soglia minima di prova.

Il **patrocinio a spese dello Stato, previsto in Italia**, può essere accessibile ai soggetti segnalanti coinvolti in procedimenti civili o penali, ma **è soggetto a limiti di reddito**, e non è automaticamente garantito.

Oltre al sostegno legale, in alcuni casi può essere riconosciuto un **supporto psicologico o finanziario**, soprattutto nei casi in cui le ritorsioni abbiano causato danni emotivi o difficoltà economiche. La legge italiana non prevede ancora un **fondo nazionale dedicato allə segnalanti**, ma alcune forme di supporto potrebbero essere attivate a livello locale o attraverso progetti europei.

In determinati casi, le autorità possono anche riconoscere formalmente lo *status* di segnalante (si veda il dettaglio seguente sulle certificazioni).

Accesso ai centri di informazione e supporto

Per tutelare ulteriormente lə segnalanti, come già ricordato in questa guida (capitoli 1 e 2), gli Stati membri sono invitati dalla Direttiva a istituire i "centri d'informazione", ossia **servizi di consulenza indipendenti** che possano fornire **assistenza, orientamenti pratici, competenza, ascolto, informazioni e sostegno** a segnalanti potenziali o che si trovano a subire ritorsioni. Ove esistenti, lə segnalanti possono quindi rivolgersi a tali servizi per ricevere una consulenza riservata sui loro diritti, sui rimedi disponibili e

[63] *Tribunale di Milano, Sezione Lavoro, Sentenza n. 3854 del 13 dicembre 2023; Corte d'Appello di Milano, Sentenza n. 252 del 3 marzo 2023. Si veda: https://transparency.it/images/whistleblowing/report/2023/fascicoli/Rassegna_giurisprudenziale.pdf*

sulle opzioni legali. Tali strutture sono progettate per offrire un supporto diretto e ove possibile immediato, intercettando lə segnalanti potenziali e facendo in modo che possano affrontare il processo di segnalazione e protezione in modo sicuro, sereno e informato, garantendo come esito finale un buon *report* di segnalazione.

Ai sensi della Direttiva, **questi servizi possono essere forniti sia da istituzioni pubbliche che da enti civici qualificati**. Nel caso italiano, si evidenzia come l'ANAC, nel giugno 2024 e in attuazione alle previsioni previste dal'art. 18 della legge nazionale di recepimento, ha predisposto una pagina, accessibile dal portale dell'autorità (come indicato anche nel capitolo 1), che contiene un elenco di associazioni le quali si sono impegnate (procedendo poi a stipulare una convenzione con ANAC stessa) a garantire tali servizi di supporto e informazione. Va comunque ricordato come il caso italiano abbia meritevolmente recepito una prassi preesistente: esistono infatti esempi di accompagnamento che anticipano la Direttiva. Due esempi storici sono quello fornito da *Transparency international* **Italia** per tramite del servizio ALAC[64], attivo dal 2014, e da Libera attraverso il numero verde Linea Libera[65], dal 2017.

Cp. 1 ›

Tali strutture sono indispensabili per sottrarre lə potenziale segnalante alla fatica del sostenere, in solitudine, tutto il carico derivante sia da una fase di dilemma etico che di scrittura del *report* di segnalazione stesso. Possono pertanto fare la differenza tanto nel sostenere lo stato emotivo del soggetto segnalante e la continuazione/ripresa del suo progetto di vita senza che risenta della situazione, quanto nel garantire una buona qualità della segnalazione stessa.

Tutele da ritorsioni oltre il luogo di lavoro

Le ritorsioni contro lə segnalanti vanno oltre le conseguenze sul luogo di lavoro, come il licenziamento o il demansionamento. Possono anche includere:

A. Molestie e intimidazioni.
B. Danno reputazionale.
C. Campagne diffamatorie sui social media.
D. Liste nere del settore, che possono avere un grave impatto sulle prospettive di carriera di unə segnalante.

Pertanto, le tutele si estendono anche in queste situazioni, garantendo la protezione al di fuori del luogo di lavoro e riconoscendo che lə segnalanti possono dover affrontare conseguenze sociali più ampie.

In **Italia**, la legge garantisce esplicitamente una protezione che copre anche le ritorsioni che possono consistere in danni economici o finanziari, inclusa la perdita di opportunità economiche e il mancato guadagno; risoluzione anticipata o risoluzione del contratto di fornitura di beni o servizi;

[64] *ALAC:* https://transparency.it/alac

[65] *Linea Libera:* https://www.libera.it/it-schede-536-linea_libera

annullamento di una licenza o di un permesso; richiesta ingiustificata di esami psichiatrici o medici.

Certificazione da parte delle autorità competenti

In alcuni Stati membri, lo ***status* formale di segnalante** è un prerequisito per ricevere sostegno e misure di protezione. Viene pertanto formalmente riconosciuto tale *status*, tramite una **"Certificazione di segnalante"**, come indicato nel Considerando 90(1) della Direttiva. Tra i Paesi che hanno introdotto questa certificazione ci sono **Francia, Lettonia, Polonia e Spagna** (in particolare nella Comunità Valenzana, rilasciata dall'Agenzia per la prevenzione e la lotta contro la frode e la corruzione). In **Italia**, tale certificazione non è contemplata dall'ordinamento giuridico.

Se è vero che tale certificazione può essere utile in procedimenti giudiziari o quando si cerca assistenza da parte di istituzioni pubbliche o private, rafforzando la posizione del soggetto segnalante quando deve dimostrare il suo diritto a misure di protezione, è altrettanto vero che **potrebbe comportare un rischio o un limite.** Si pensi a possibili lentezze burocratiche o, persino, a una sorta di etichettatura ufficiale che potrebbe rendere lə segnalante facilmente identificabile come tale, con il rischio di stigmatizzazione sociale o professionale.
In questa guida, suggeriamo come tale certificazione possa essere del tutto opzionale, garantendo pertanto che, anche in assenza di essa, lə segnalanti abbiamo un accesso effettivo alle tutele.

Sostegno finanziario

La Direttiva non prevede esplicitamente un sostegno finanziario diretto per lə segnalanti. Tuttavia, si potrebbero interpretare come tale le misure compensative per i danni subiti, come il risarcimento per danni economici o non economici derivanti dalle ritorsioni, o il supporto psicologico. Siamo però lontani dalla previsione di incentivi economici utili a favorire l'emersione delle segnalazioni, come avviene, per esempio, negli Stati Uniti.

Per quanto riguarda il sostegno finanziario, **solo alcuni Paesi hanno introdotto misure specifiche nel loro quadro giuridico**. Tali misure, tuttavia, sono spesso limitate nella portata e nell'importo. Paesi come il Belgio e la Slovacchia offrono un supporto più ampio, coprendo i costi per assistenza sanitaria o psicologica privata. Tuttavia, queste forme di sostegno sono variabili e non estese a tutti i Paesi dell'Unione Europea.

Il tema del sostegno finanziario rimane quindi ancora fortemente dibattuto in ambito comunitario (e non), e non esiste una visione unitaria in merito. **Quello che suggeriamo in questa pagine è che si dovrebbero garantire i migliori sistemi e garanzie anche finanziarie, per evitare che lə segnalante paghi (anche economicamente) la scelta fatta vedendo intaccato il proprio progetto di vita.**

4.3 AMPLIAMENTO DELL'AMBITO DELLE VIOLAZIONI

Sebbene la Direttiva si concentri quasi esclusivamente sulle violazioni del diritto dell'Unione Europea, essa incoraggia gli Stati membri a **prendere in considerazione l'estensione delle tutele anche alle violazioni del diritto nazionale e a comportamenti non etici** che, pur non essendo formalmente illeciti, comportano rischi per la società o il sistema economico. Questo approccio lascia **agli Stati membri un margine di discrezionalità** nell'ampliare l'ambito delle violazioni oggetto di segnalazione, al fine di tutelare lə segnalanti anche in caso di comportamenti che, pur non configurando reati, possano comunque compromettere l'interesse pubblico, la buona amministrazione o la democrazia.

A riguardo, **in Italia la precedente normativa sul *whistleblowing***, introdotta con la Legge 179/2017 antecedente alla Direttiva, **aveva già previsto la protezione dellə segnalanti** da ritorsioni in caso di denuncia di illeciti all'interno della pubblica amministrazione e delle società a partecipazione pubblica. Tale normativa aveva già introdotto il concetto di **malamministrazione come oggetto delle segnalazioni**, riconoscendo che le segnalazioni possono riguardare illeciti, ma anche pratiche scorrette che danneggiano l'efficienza o l'integrità delle istituzioni pubbliche, alle quali è possibile rispondere anche con un'eventuale azione organizzativa dell'ente. Il ***whistleblowing***, in tale impianto, non implicherebbe quindi la sola segnalazione di illeciti, ma riguarderebbe anche la possibilità di **sollevare una questione o di evidenziare una irregolarità**, portando all'attenzione situazioni che, pur non essendo illegali, possano compromettere l'interesse pubblico o la buona gestione amministrativa.

Nel caso italiano, una questione da attenzionare riguarderebbe quindi l'ambito delle violazioni oggetto di segnalazione: secondo alcune interpretazioni, quello fissato dalla normativa del 2017 risulterebbe più ampio rispetto a quanto previsto dalla Direttiva e dalla legge di recepimento. Si tratta di una partita interpretativa ancora aperta, in quanto una volta introdotte norme di protezione superiori, secondo il principio giuridico del "non regresso", non dovrebbe essere possibile retrocedere a uno stadio meno favorevole, impedendo che le tutele per lə segnalanti vengano abbassate. In coerenza di ciò, anche l'ANAC ha comunque sottolineato che gli atti di malamministrazione possano essere indici di illeciti, riportando così la tutela a comportamenti scorretti che possano danneggiare la buona amministrazione, anche se non configurano illeciti.

Questo approccio dovrebbe consolidarsi come prassi anche a livello comunitario, pur in funzione delle esigenze locali.

Guardando oltre confine, anche in **Spagna** la protezione offerta allə segnalanti si estende a coloro che denunciano non solo le azioni od omissioni previste dalla Direttiva, ma anche quelle che, secondo il diritto spagnolo, potrebbero costituire reati o violazioni amministrative gravi. Inoltre, la legge spagnola copre anche reati o illeciti amministrativi gravi che comportano una perdita economica per lo Stato e per la sicurezza sociale (Legge 2/23 Art. 2.1.b).

FOCUS GENERE

La protezione dellə segnalanti richiede un approccio inclusivo, riconoscendo che gli individui appartenenti a **gruppi emarginati** o coloro che si trovano ad affrontare vulnerabilità intersezionali possono sperimentare **un rischio maggiore di ritorsioni** e una maggiore paura rispetto ad altrə. Il rischio di ritorsioni può influenzare se e come una persona decide di denunciare. Le ricerche, compresi gli studi condotti da *Transparency International,* confermano che le donne possono provare maggiore paura e stress quando denunciano comportamenti scorretti (cfr. **capitolo 5**, approfondimento sul genere).

Cp. 5 >

Uno dei principali fattori che influenzano la decisione delle donne di segnalare o denunciare una cattiva condotta è la dinamica di potere sul posto di lavoro:

A. Squilibri di potere all'interno dell'organizzazione: gli ambienti di lavoro sono spesso dominati da uomini in posizioni di potere e autorità decisionale. Maggiore è lo **squilibrio di potere tra uomini e donne**, maggiore è il rischio di ritorsioni per le donne che segnalano.
B. Le ritorsioni contro le donne spesso prendono di mira la loro sfera personale: a differenza di altre forme di ritorsione, le donne possono subire **attacchi intimi e personali, come commenti sessisti o molestie di genere.**
    I. Bulgaria: le organizzazioni della società civile hanno espresso preoccupazione per il crescente numero di azioni legali contro le donne che denunciano o segnalano illeciti nel giornalismo. Le giornaliste sono spesso percepite come il sesso debole, il che le rende bersagli più facili per l'intimidazione e le tattiche di paura.
C. Impatto sulla salute e psicologico: la ricerca mostra che le donne prendono **il congedo per malattia** più frequentemente degli uomini dopo aver segnalato una cattiva condotta, spesso come un modo per evitare ritorsioni sul posto di lavoro.
    I. Italia: gli studi hanno evidenziato che gli svantaggi affrontati dalle donne nel *whistleblowing* si manifestano anche come **una minore consapevolezza dei loro diritti** e una ridotta capacità di proteggersi nei procedimenti giudiziari.

Per affrontare queste sfide di genere, le organizzazioni dovrebbero:

Cp. 1 >

A. **Sviluppare e approvare protocolli sensibili al genere** (cfr. **capitolo 1** approfondimento sul genere):
    I. Con il consenso e un'adeguata rappresentanza, le organizzazioni dovrebbero stabilire protocolli o linee guida specifici per la gestione dei casi di *whistleblowing* legati al genere.
    II. Assicurarsi che questi protocolli siano integrati sia nelle politiche di protezione dellə segnalanti che nelle politiche di uguaglianza e non discriminazione dell'organizzazione.
    III. Questi protocolli dovrebbero delineare procedure chiare per segnalare, indagare e affrontare i casi di violenza, molestie o discriminazioni di genere.
    IV. Tutti gli individui dovrebbero essere pienamente informati dei loro diritti e dei servizi di sostegno disponibili.
B. **Ampliare l'accesso al patrocinio a spese dello Stato, al supporto psicologico e ai servizi esterni:**
    I. Garantire che l'assistenza legale sia ampiamente disponibile per le donne e altri gruppi esposti alla discriminazione, in modo che possano difendersi meglio da ritorsioni e azioni legali.
    II. Garantire che i meccanismi di segnalazione siano concepiti per prevenire ritorsioni e vittimizzazione secondaria nei casi basati sul genere, assicurando che le segnalazioni non siano accessibili a persone all'interno della stessa gerarchia sul luogo di lavoro, come supervisori o colleghi. Lə segnalanti devono sentirsi sicurə che la loro identità e le loro azioni saranno protette, soprattutto nei casi sensibili basati sul genere in cui il rischio di ritorsioni è più elevato.
    III. Fornire informazioni sui servizi di sostegno esterni, sul patrocinio a spese dello Stato, sul sostegno psicologico e su altre organizzazioni di difesa di vittime di reati aspecifici (in Italia, per esempio, rete Dafne). Ciò consente a potenziali segnalanti di sentirsi più sicurə e informatə quando valutano se segnalare una cattiva condotta e di affrontare eventuali sfide che potrebbero incontrare durante il processo.

4.4 DIVULGAZIONE AL PUBBLICO E SITUAZIONI DI EMERGENZA

Circa le protezioni che si attuano a chi sceglie il canale della divulgazione pubblica, la premessa è che, in generale, lə segnalanti, anche ai fini di una loro più efficace della stessa tutela, sono incoraggiatə a effettuare una segnalazione interna o esterna, prima di rendere pubblica la loro divulgazione. Tuttavia, la Direttiva riconosce che, **in determinate circostanze, la divulgazione pubblica può essere necessaria, quindi protetta**. Secondo la Direttiva (Art. 15), tali circostanze si verificano quando è necessario agire tempestivamente per proteggere un interesse pubblico fondamentale, come nel caso di minacce imminenti o danni gravi. Questi possono includere, per esempio, disastri ambientali, rischi per la salute, frodi finanziarie, o situazioni in cui le prove possono essere distrutte o le autorità coinvolte venire compromesse, richiedendo dunque tempestività. In tali casi, si dice che la divulgazione pubblica risulta coerente col principio di proporzionalità.

Il principio di proporzionalità implica che la divulgazione al pubblico debba essere una misura commisurata alla gravità della minaccia e all'urgenza della situazione. In altre parole, lə segnalante deve ritenere che la divulgazione pubblica sia l'unica opzione possibile e adeguata per prevenire danni immediati. Si tratta quindi di una sorta di procedura emergenziale, per situazioni emergenziali. Questo principio assicura che la divulgazione non sia eccessiva rispetto al rischio, e che non vengano fatte azioni che possano danneggiare in modo ingiustificato le parti coinvolte o l'istituzione, quando altre vie di segnalazione (come quella interna o esterna) possano essere altrettanto efficaci. **Tuttavia, è una grossa sfida,** per lə segnalante potenziale, **comprendere se effettivamente sta agendo in modo proporzionato.** Essendo spesso espostə a informazioni complesse o trovandosi a dover far fronte a una complessa gestione delle emozioni corrispondenti, lə segnalante potrebbe percepire un rischio imminente e agire di conseguenza. Per tale ragioni è essenziale che essə, prima di fare una divulgazione pubblica, sia accompagnatə al fine di valutare attentamente la situazione, magari consultando previamente servizi di supporto e informazione per determinare se altre soluzioni, come la segnalazione interna o esterna, potrebbero essere altrettanto efficaci per tutelare l'interesse pubblico senza danneggiare ingiustificatamente altre parti.

Nel contesto spagnolo, per esempio, i soggetti segnalanti che effettuano una divulgazione pubblica devono soddisfare requisiti specifici per ottenere protezione. Questi requisiti non sono generici, ma devono essere conformi a criteri legali precisi, come previsti dalla legge spagnola, che riflette l'importanza di garantire che la divulgazione sia fatta in maniera giustificata e proporzionata. **In Italia, la protezione dellə segnalanti in caso di divulgazione pubblica è soggetta al suddetto principio di proporzionalità**, e le autorità competenti devono valutare se le circostanze giustificano una divulgazione pubblica rispetto a una segnalazione interna o esterna. In entrambi questi Paesi, quindi, la divulgazione pubblica deve essere una risposta proporzionata a una minaccia grave e imminente, e lə segnalante dovrebbe agire senza abusare di questo strumento.

4.5 PERDITA DI PROTEZIONE

La protezione può essere revocata in presenza di condizioni specifiche, come il rischio di abuso del sistema da parte di segnalanti, per garantire che il meccanismo di *whistleblowing* rimanga uno strumento responsabile e trasparente, evitando che venga utilizzato in modo fraudolento o per scopi non corretti. In dettaglio, la protezione non si estende quando ci si ritrova davanti a una di queste situazioni:

A. **Segnalazioni dannose**: lə segnalanti che forniscono consapevolmente e intenzionalmente informazioni false o fuorvianti perdono la loro protezione. Gli Stati membri possono imporre sanzioni per tali casi.
B. **Mancato rispetto delle procedure**: la segnalazione al di fuori dei canali designati comporta in genere la perdita della protezione, tranne in caso di minacce urgenti o distruzione delle prove.
C. **Attività illegali**: lə segnalanti coinvoltə in *hacking*, furto di dati o accesso non autorizzato non sono protettə per garantire un uso responsabile del sistema.
D. **Violazione della riservatezza**: se lə segnalante divulga informazioni eccessive o sensibili senza giustificazione, la protezione può essere revocata.
E. **Divulgazione pubblica impropria**: lə segnalanti devono prima tentare di effettuare segnalazioni interne o esterne, a meno che non vi sia una valida giustificazione per una urgente esposizione pubblica.

4.6 CHI OFFRE TUTELE E SUPPORTO ALLƎ SEGNALANTI (E COME VIENE A SUA VOLTA TUTELATƎ)

La Direttiva (al Considerando n. 41 e poi all'Art. 4) estende le tutele anche a coloro che, a diverso titolo e per ragioni differenti, assistono lə segnalanti, garantendo che tutti i soggetti coinvolti possano operare in modo sicuro ed efficace. Non sempre ciò è stato però previsto nelle normative nazionali di recepimento. Vediamo come.

Facilitatorə

Lə facilitatorə, come consulenti legali e rappresentanti sindacali, aiutano a segnalare le violazioni in modo sicuro. Il loro ruolo comprende:

A. Fornire supporto informale o assistenza legale.
B. Aiutare a perfezionare i report per garantire l'accuratezza.
C. Garantire il rispetto delle procedure di segnalazione
D. Aiutare a utilizzare correttamente i canali di segnalazione interni.
E. Mantenere la riservatezza dellə segnalante.

L'Art. 2.1 della legge italiana definisce lə facilitatore come "la persona che assiste lə segnalante nel processo di segnalazione, operando nello stesso contesto e la cui assistenza deve essere riservata". Allo stesso tempo, **la norma nazionale prevede che la protezione si estenda allə facilitatorə stesso.** Rispetto alla Direttiva, che non impone alcun vincolo di

appartenenza al medesimo contesto lavorativo, il legislatore italiano ha introdotto una limitazione significativa, restringendo di fatto il novero dei soggetti qualificabili come facilitatorə e riducendo l'ampiezza della tutela prevista a livello europeo.

L'Art. 5 della Legge bulgara stabilisce che la protezione è concessa anche alle "persone che assistono lə segnalante nel processo di segnalazione e la cui assistenza è riservata". La legge però non si riferisce a queste persone definendole espressamente "facilitatorə" e non fornisce alcun dettaglio su cosa possa consistere in questa assistenza.

Alla luce di questi due esempi, appare evidente come **la figura del facilitatorə richiederà, in futuro, una definizione più chiara e compiuta**, magari anche sulla base delle prassi che emergeranno. Ciò sarà utile per estendere e armonizzare il suo ruolo con altre forme di supporto, come quelle offerte dai centri di informazione e assistenza (si veda sotto), evitando sovrapposizioni o contrapposizioni.

Organizzazioni del terzo settore (e centri civici di supporto)

Le ONG e i gruppi della società civile possono:

A. **Offrire sostegno allə potenziali segnalanti, fungendo dai già più volte citati centri di informazione**, tramite l'offerta di consulenza pratica sulla segnalazione, le tutele e sui diritti correlati, di assistenza nella segnalazione, di supporto psicologico per aiutare lə segnalanti a gestire lo stress e il contraccolpo sociale, di informazioni sul come ottenere il patrocinio gratuito.
B. **Offrire canali sicuri e visibilità per il canale della divulgazione pubblica**, facilitando l'accesso ai *media* o consentendo la pubblicazione attraverso piattaforme indipendenti.

Se quindi è vero che le associazioni del terzo settore figurano come realtà che possono offrire un'utile misura di supporto (in quanto centri di informazione), allo stesso modo la Direttiva, al Considerando 89, riporta come le "persone che forniscono supporto allə segnalanti, come sindacati o organizzazioni della società civile, possono anch'esse essere oggetto di ritorsioni e dovrebbero quindi beneficiare di protezione, almeno quando l'assistenza è fornita in modo riservato".
Le associazioni del terzo settore, nell'espletare tale ruolo, sono infatti loro stesse vulnerabili alle ritorsioni: inserimento in *blacklist*, minacce legali, esclusione da finanziamenti pubblici e privati, ostacoli burocratici, boicottaggio da parte di *partner* e collaboratori, diffusione di informazioni false, sabotaggio e disturbo delle loro attività.

In Italia, però, il legislatore nazionale ha omesso di estendere le tutele, previste per lə facilitatorə, **anche agli enti civici che forniscono supporto**, i quali pertanto non godono, a oggi, di alcuna protezione.

In questa guida, ricordiamo l'importanza di garantire tutele anche a chi offre supporto a segnalanti. **Nei contesti in cui le leggi nazionali non sono**

ancora pienamente allineate alla Direttiva, suggeriamo di intervenire tempestivamente per riformare l'impianto normativo.

Autorità competenti

Come già detto (cfr. **capitolo 4.2.1**) le Autorità, per come previsto dalla Direttiva, esercitano un ruolo chiave nel guidare lə segnalanti sulle procedure di segnalazione, informare circa i meccanismi di protezione, ove previsto certificare lo *status* di segnalante.

La Direttiva non prevede esplicitamente la protezione per le Autorità da ritorsioni. Tuttavia, in quanto autorità pubbliche, si dà per scontato che beneficino di una protezione implicita legata al proprio ruolo istituzionale e alle leggi generali sulla protezione degli enti pubblici. Anche nelle normative di recepimento di **Italia**, **Bulgaria** e **Spagna** non c'è una norma specifica che tuteli l'ente dalle ritorsioni connesse al suo compito di gestione del canale di segnalazione.

FOCUS GOVERNO APERTO

Protezione dellə segnalanti

Una protezione efficace dellə segnalanti trarrebbe vantaggio da sforzi coordinati tra diversi attori quali istituzioni, organizzazioni dei media, gruppi della società civile, sindacati e organismi per i diritti umani. Questo approccio collaborativo riconosce il ruolo cruciale dellə segnalanti in tutti i settori e rafforza la narrativa che collega la loro segnalazione e protezione con i diritti dellə lavoratori e la libertà di espressione. Questa connessione è particolarmente rilevante nei Paesi che registrano un aumento delle cause legali strategiche contro la partecipazione pubblica (SLAPP).

Gli operatori di tutti i settori hanno indicato che quando la Direttiva viene attuata attraverso la creazione di nuove autorità o uffici dedicati responsabili del *whistleblowing*, **l'impegno multilaterale può essere decisivo per creare fiducia tra tutte le parti coinvolte**, soprattutto se effettuato nel quadro dell'attuazione dei Piani d'Azione Nazionali di governo aperto del Paese. Processi come quelli dell'*Open Government Partnership* (OGP) offrono un'utile piattaforma per questo dialogo *multi-stakeholder*. In particolare, ciò può contribuire ad approfondire ulteriormente la partecipazione dei rappresentanti del settore privato, sia come enti individuali che attraverso organismi rappresentativi, e quindi contribuire a una discussione più equilibrata e a meccanismi di protezione più efficaci.

Un coinvolgimento significativo delle parti interessate dovrebbe estendersi anche **alla partecipazione a consessi internazionali come la Convenzione delle Nazioni Unite contro la corruzione (UNCAC).** Ciò include la garanzia che lə segnalanti stessə, nonché le organizzazioni che si occupano della loro protezione, siano attivamente coinvoltə nelle delegazioni nazionali e nelle discussioni preparatorie. Un forte esempio di questo approccio è stato visto alla decima conferenza degli Stati firmatari dell'UNCAC (CoSP10) ad Atlanta[66], dove la risoluzione sulla protezione delle persone segnalanti è stata guidata da un ex segnalante che è stato direttamente incluso nella delegazione serba. Ciò dimostra il valore di incorporare la prima esperienza dei soggetti nel processo decisionale, garantendo che coloro che hanno subito ritorsioni o hanno affrontato il processo di segnalazione contribuiscano a definire protezioni più efficaci. **Integrando lə segnalanti e i gruppi di**

[66] *Si veda:* https://whistleblowingnetwork.org/News-Events/News/News-Archive/Governments-Around-the-World-Step-Up-to-Support-Wh

difesa nelle delegazioni ufficiali, nei gruppi di lavoro e nei processi di negoziazione, **i Paesi possono sviluppare politiche non solo ben informate, ma anche pratiche e applicabili.** Questo approccio inclusivo migliora la legittimità, rafforza la cooperazione internazionale e garantisce che i quadri di protezione dei segnalanti siano radicati nelle sfide e nelle esigenze del mondo reale.

Oltre a queste misure di collaborazione, le organizzazioni della società civile raccomandano vivamente un'**interpretazione estensiva delle leggi** sulla protezione dellə segnalanti, che vada oltre le disposizioni della Direttiva e apra la strada alla sua futura riforma.

A. Una proposta fondamentale consiste nell'estendere le garanzie alle **organizzazioni che forniscono sostegno e consulenza allə segnalanti**, garantendo che coloro che assistono le persone segnalanti siano anche protettə da minacce e ritorsioni. I governi e la società civile possono collaborare a questa espansione, riconoscendo il ruolo cruciale che queste organizzazioni svolgono nel consentire un'informativa sicura ed efficace.
B. Un altro passo fondamentale è il raggiungimento **di una maggiore armonizzazione** tra i meccanismi di protezione dellə segnalanti e altri quadri giuridici, come quelli concepiti per i **programmi di protezione dellə testimoni e le segnalazioni in relazione alla corruzione che coinvolge gruppi criminali organizzati.** Un approccio più integrato contribuirebbe a garantire che le persone che segnalano illeciti ricevano adeguate misure di sicurezza.
C. Pur non essendo esplicitamente contemplate dalla Direttiva, le organizzazioni della società civile sostengono l'estensione della protezione ai casi in cui la cattiva condotta o la corruzione sono smascherate attraverso l' **accesso alle informazioni pubbliche**. Ciò include le rivelazioni effettuate da **giornalistə, ONG, avvocati e cittadinə attivə** che, nell'interesse pubblico, scoprono e segnalano irregolarità.

Diversi strumenti internazionali supportano questa interpretazione più ampia della protezione dei segnalanti. La stessa Direttiva (UE) 2019/1937, la Legge europea sulla libertà dei media (EMFA) e la Convenzione delle Nazioni Unite contro la corruzione (UNCAC) con le relative risoluzioni, contribuiscono a creare un contesto giuridico più favorevole per l'ampliamento e l'armonizzazione delle garanzie. Rafforzando le tutele legali e ampliandone la portata, i governi possono migliorare la trasparenza, incoraggiare la responsabilità e creare condizioni più sicure per coloro che segnalano gli illeciti sia nel settore pubblico che in quello privato.

Supporto allə segnalanti

Un'iniziativa positiva di governo aperto a sostegno dellə potenziali segnalanti è quella di istituire un **registro pubblico delle OSC che forniscono servizi gratuiti di supporto e consulenza**, per migliorarne il riconoscimento e la visibilità. Nel caso dell'Italia, questo obiettivo è stato raggiunto inserendo l'impegno nel suo 5° Piano d'Azione Nazionale (5NAP) per il governo aperto (2021-2023).[67] Per chi volesse replicare l'iniziativa italiana, si consiglia di:

A. **Definire i requisiti per l'iscrizione delle OSC nell'elenco pubblico**, per garantire l'imparzialità, il rispetto delle norme sulla privacy e la competenza.
B. **Promuovere competenze professionali diversificate** all'interno delle OSC per garantire un supporto olistico (legale, psicologico, ecc).
C. **Prevedere una convenzione formale con l'autorità** per le organizzazioni della società civile idonee.
D. **Mantenere attivo un gruppo di lavoro tra i membri dell'albo** per monitorare le esigenze di formazione e informazione e facilitare lo scambio tra pari.
E. **Istituire *forum* almeno semestrali per affrontare le sfide** sistemiche cui devono far fronte le organizzazioni della società civile e le preoccupazioni derivanti da casi reali, nel rispetto della tutela della riservatezza.
F. **Incoraggiare o richiedere a tutti gli enti pubblici di seguire l'esempio dell'autorità** nel rendere visibile l'elenco anche sul proprio sito *web* e nella comunicazione allə proprə dipendenti.

Un'ulteriore misura avanzata nell'ambito di un governo aperto consiste nell'istituire un coordinamento e una messa in rete tra enti di consulenza e supporto riconosciuti per

[67] *Si veda:* https://www.opengovpartnership.org/members/italy/

garantire che lə potenziali segnalanti siano indirizzati all'organizzazione più adatta per ricevere orientamento. Per esempio, **si potrebbe creare un *hub* centralizzato** per raccogliere e valutare le esigenze dellə segnalanti, per poi indirizzarlə all'organizzazione di supporto appropriata sulla base di competenze territoriali o settoriali. Ciò contribuirebbe a semplificare il processo e a garantire che le persone ricevano l'assistenza più efficace.

Tali servizi di assistenza legale e psicologica dovrebbero essere gratuiti per lə potenziali segnalanti, al fine di rimuovere eventuali ostacoli economici all'accesso ai servizi. A tal fine, il governo dovrebbe garantire **finanziamenti pubblici per sostenere le organizzazioni** (istituzionali e civiche) e **assistenza legale gratuita** per lə segnalanti in caso di processo.

4.7 RACCOMANDAZIONI

Per offrire un supporto e una protezione completi alle persone che accedono alle procedure di segnalazione, è di fondamentale importanza promuovere un approccio efficace e collaborativo al *whistleblowing*. Ciò richiede il coinvolgimento di più parti interessate, ognuna delle quali contribuisce con la propria esperienza e il proprio ruolo nell'affrontare le sfide associate al *whistleblowing*.

Le misure chiave per migliorare il supporto e la protezione dellə segnalanti includono:

1. MIGLIORARE L'ACCESSO AL SUPPORTO DEI WISTLEBLOWER

I soggetti pubblici e privati dovrebbero migliorare l'accessibilità pubblicando elenchi delle organizzazioni della società civile (OSC) e di altri organismi pertinenti che offrono assistenza e informazioni allə potenziali segnalanti.

2. PROMUOVERE UNA COOPERAZIONE CONTINUA

La cooperazione continua tra le autorità competenti, le organizzazioni della società civile e le altre organizzazioni pertinenti è fondamentale per garantire che siano ben attrezzate per fornire servizi di alta qualità allə segnalanti.

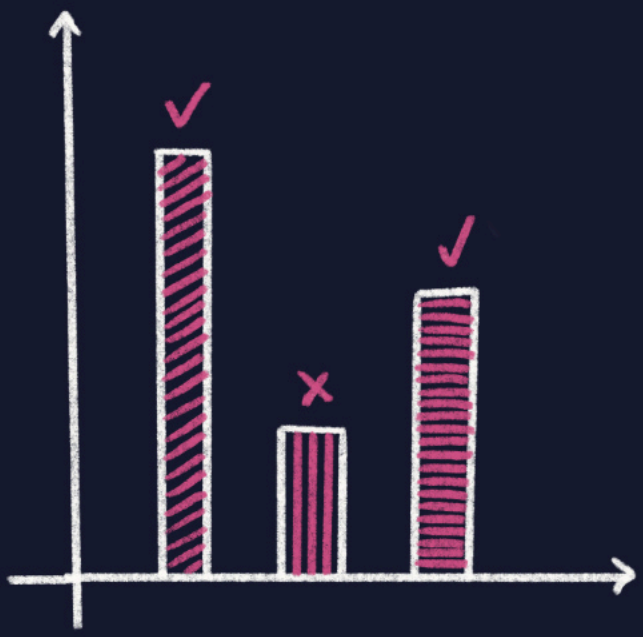
3. MIGLIORARE LE INIZIATIVE DI CONSAPEVOLEZZA E FORMAZIONE

Le amministrazioni e le aziende devono promuovere attivamente **iniziative di sensibilizzazione e programmi di formazione** per migliorare la comprensione delle normative e delle procedure di *whistleblowing*. Inoltre, dovrebbero essere attuati corsi di formazione mirati per lə funzionarə pubblicə al fine di sviluppare le migliori pratiche per la gestione delle segnalazioni di irregolarità e la gestione efficace dei relativi processi.

4. FACILITARE IL DIALOGO ATTRAVERSO INCONTRI DEDICATI

Infine, l'organizzazione di incontri dedicati con rappresentanti del settore pubblico e privato può **facilitare un dialogo costruttivo,** consentendo agli *stakeholder* di affrontare sfide comuni e identificare soluzioni ottimali in modo collaborativo.

Valutazione dell'efficacia del sistema di segnalazione e dello sviluppo di una cultura del *whistleblowing*



Capitolo 5

Open the whistle

VALUTAZIONE DELL'EFFICACIA DEL SISTEMA DI SEGNALAZIONE E DELLO SVILUPPO DI UNA CULTURA DEL *WHISTLEBLOWING*

Capitolo 5

5.1 MISURARE CIÒ CHE CONTA: EFFICACIA, CONSAPEVOLEZZA E ADATTAMENTO CULTURALE

Ultimo aspetto che abbiamo scelto di affrontare in questa guida riguarda la **misurazione e valutazione periodica dell'efficacia e dell'impatto dei sistemi di segnalazione**, nonché il livello di consapevolezza e comprensione del processo di *whistleblowing*.

Se è vero che l'istituto abbia già affrontato importanti sfide (dai ritardi nel recepimento della Direttiva da parte della maggior parte degli Stati membri, l'integrazione incompleta nei sistemi giuridici nazionali e la complessità del quadro normativo), quello della **valutazione dell'efficacia di questi sistemi (così come dei fattori culturali che ne influenzano il successo) è un fronte determinante ai fini della creazione di un sistema di fiducia attorno a esso.**

La premessa è che occorre valutare **i sistemi di *whistleblowing* non solo come strumenti di *compliance*, ma come meccanismi integrali atti a promuovere comportamenti etici e integrità organizzativa**.

La ricerca e la pratica contemporanee evidenziano la necessità di metodi di valutazione completi per garantire che i canali di *whistleblowing* siano accessibili, affidabili ed efficaci nell'affrontare gli illeciti, proteggendo al contempo i soggetti segnalanti da ritorsioni. Inoltre, la dimensione culturale, che comprende la fiducia, la consapevolezza e la disponibilità dei dipendenti a segnalare, è emersa come una pietra miliare nella creazione di una **cultura proattiva della segnalazione.**

5.2 REVISIONE DEGLI STRUMENTI DI MISURAZIONE E VALUTAZIONE ESISTENTI

5.2.1 Organizzazione internazionale per la standardizzazione

Il framework ISO 37002:2021 è una guida internazionale che aiuta, nell'elaborazione delle politiche e offre approfondimenti sull'implementazione dei sistemi di gestione del *whistleblowing*, in diverse istituzioni[68]. Le linee guida si basano su tre principi fondamentali: fiducia, imparzialità e protezione, i quali garantiscono che il sistema funzioni correttamente e che chi segnala sia protettə da ritorsioni. Il *framework* descrive quattro passaggi chiave per gestire efficacemente le segnalazioni di illeciti:

A. **Ricezione delle segnalazioni**: garantire che le segnalazioni vengano raccolte in modo sicuro e confidenziale.
B. **Valutazione delle segnalazioni**: esaminare con attenzione ogni segnalazione per determinare se è necessaria un'indagine.
C. **Gestione delle segnalazioni**: seguire un processo chiaro per affrontare le segnalazioni, rispettando i diritti di tutte le parti coinvolte.
D. **Chiusura dei casi**: fornire una risoluzione finale in modo trasparente e documentato, garantendo che tutte le azioni siano adeguatamente seguite.

Progettate per essere universalmente applicabili, queste linee guida sono rilevanti per organizzazioni di tutte le dimensioni, tipi e settori, compresi gli enti pubblici, privati e senza scopo di lucro.

Il quadro fornisce un approccio standardizzato alla valutazione dei sistemi di *whistleblowing*, con l'obiettivo di facilitare il miglioramento delle politiche e della *governance*. I casi studio esistenti evidenziano che l'attuazione di questo *standard* per i sistemi di gestione delle segnalazioni è spesso parziale e richiede un ulteriore sviluppo in aree specifiche, come le politiche di sensibilizzazione e protezione delle persone segnalanti. Di conseguenza, **potrebbe essere necessario adattare il quadro per soddisfare esigenze organizzative specifiche.**

5.2.2 Piattaforme di comunicazione digitale

La legge sui servizi digitali[69] introduce strumenti per creare uno spazio online più sicuro, più equo e più trasparente nell'UE[70] . Tra questi c'è lo strumento *DSA whistleblower*, che consente di identificare pratiche dannose di piattaforme online molto grandi e motori di ricerca *online*

---

[68] *Organizzazione internazionale per la standardizzazione, ISO 37002:2021. Sistemi di gestione del whistleblowing - Linee guida: https://www.iso.org/obp/ui/en/#iso:std:65035:en*

[69] *Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (legge sui servizi digitali): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065*

[70] *Commissione Europea. Strumento per i segnalanti della legge sui servizi digitali: segnalazione di informazioni privilegiate sulle piattaforme online: https://digital-services-act-whistleblower.integrityline.app*

(VLOP/VLOSE).[71] Fornisce un canale sicuro e, facoltativamente, anonimo per la comunicazione alla Commissione Europea di informazioni interne (quali relazioni, note, scambi di messaggi di posta elettronica, metriche di dati, ricerche interne, decisioni e altre circostanze pertinenti, passate, presenti o future).

Tuttavia, l'ambito della segnalazione è limitato alle pratiche che violano gli obblighi della legge sui servizi digitali, come la moderazione dei contenuti, il funzionamento dei sistemi raccomandati, la pubblicità, la valutazione e l'attenuazione dei rischi relativi ai diritti fondamentali dellə utenti, alle preoccupazioni per la sicurezza e la salute pubblica, al discorso civile, ai processi elettorali e ai diritti dellə minori. **Sebbene le piattaforme digitali migliorino l'accessibilità e l'efficienza della comunicazione, il loro limite risiede nell'offrire una comunicazione su una gamma ristretta di questioni.** Inoltre, il loro utilizzo e la loro efficacia dipendono fortemente dall'accettazione e dalla fiducia dellə utenti nel sistema.

5.2.3 Indagini empiriche: esperienze polacche e italiane

Nel dicembre 2022 è stata condotta **un'indagine empirica tra alcunə professionisti delle risorse umane, dirigenti e amministratorə in Polonia,** prima dell'entrata in vigore della legge polacca sullə segnalanti (avvenuta il 25 settembre 2024). L'indagine si è concentrata sul *whistleblowing* nel contesto più ampio del rischio per il personale, analizzando gli atteggiamenti dellə *manager* riguardo al rischio, le fonti di rischio per il personale, l'efficacia dei sistemi di *compliance* (inclusi appunto i meccanismi di *whistleblowing*) e i comportamenti e le perdite legati ai rischi derivanti dal fattore umano.

Per raccogliere i dati, sono stati utilizzati sia il metodo CAWI (*Computer-Assisted Web Interviewing*) che il metodo CATI (*Computer-Assisted Telephone Interviewing*). Sono state applicate analisi statistiche, come il test del chi-quadrato con correzione di Yates e il test di Kruskal-Wallis, per valutare le differenze nelle valutazioni dei processi di *whistleblowing* in relazione a variabili come la posizione lavorativa, le dimensioni dell'azienda, la forma di proprietà e il settore industriale

I principali risultati dell'indagine polacca sono:

A. Il *whistleblowing* è ampiamente considerato uno strumento importante sia per rilevare illeciti nelle organizzazioni che per un'efficace gestione della compliance[72].
B. Un terzo dellə intervistatə non ha un'opinione chiara sull'efficacia di sistemi di *whistleblowing* consolidati.
C. Nelle aziende di medie dimensioni, lə intervistatə hanno fornito

[71] *Commissione Europea. Vigilanza sulle piattaforme online di dimensioni molto grandi e sui motori di ricerca designati nell'ambito della legge sui servizi digitali: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-lqfbha7w*

[72] *Ibid.*

valutazioni più elevate per i canali interni di *whistleblowing* e le protezioni contro le ritorsioni rispetto ad altre organizzazioni. Le differenze nei punteggi in base alla posizione lavorativa possono essere attribuite alle variazioni della cultura organizzativa, alla fiducia dellə dipendenti nell'efficacia dei sistemi di *whistleblowing*, all'entità degli illeciti segnalati e all'adeguatezza dei canali interni.

In media, lə professionistə hanno valutato i sistemi di *whistleblowing* delle loro organizzazioni più bassi rispetto agli altri. Lə professionistə delle risorse umane, lə *manager* e lə direttorə delle risorse umane non sono d'accordo nella loro valutazione dell'attuale livello di fiducia dellə dipendenti nel corretto funzionamento e nell'affidabilità dei sistemi di *whistleblowing* delle loro aziende[73].

Uno studio empirico parallelo è stato condotto in Italia dalla Scuola Nazionale dell'Amministrazione (SNA) nell'ambito del progetto "***Training for Change*: amministrazione aperta e modelli di formazione innovativi per l'implementazione efficiente del *whistleblowing*"**[74]. L'obiettivo era quello di valutare l'impatto dei programmi di formazione SNA sulla percezione del *whistleblowing*, dato il suo relativamente debole radicamento nella cultura giuridica e organizzativa italiana. Lo studio italiano ha utilizzato una metodologia simile all'indagine polacca, adoperando sia tecniche CAWI che CATI. I dati sono stati raccolti da un campione di professionisti delle risorse umane, manager e funzionari pubblici, applicando anche in questo caso analisi statistiche come il test del chi-quadrato con correzione di Yates e il test di Kruskal-Wallis per esaminare le differenze in base alla posizione lavorativa, alla struttura organizzativa e al settore.

I principali risultati dell'indagine italiana sono:

A. **La formazione svolge un ruolo cruciale** non solo nella diffusione della consapevolezza e della conoscenza sul *whistleblowing*, ma anche nel trasformare la percezione che ne ha il pubblico.
B. **La fiducia e le barriere culturali rimangono sfide importanti** nonostante le tutele legali.
C. **Il ruolo di supporto delle organizzazioni della società civile è sottoutilizzato** e poco conosciuto (prima della formazione solo il 13% dellə intervistatə era consapevole del proprio ruolo, dopo la formazione la percentuale è salita al 46,6%).
D. **I canali interni sono meno preferiti** (38% dellə intervistatə) e molti preferiscono l'uso del canale esterno (61%) perché considerato più affidabile, indipendente ed efficace.
E. **Gli incentivi principali per segnalare illeciti sono**: protezione da ritorsioni (74,2% donne, 67,9% uomini), garanzie di riservatezza (68,5% donne, 67% uomini), sapere che l'attività segnalata sarà affrontata (59,2% donne, 57,8% uomini) e sapere che la questione che ho sollevato è considerata importante/grave (41,7% donne, 46,4% uomini).

---

[73] *Ibid.*

[74] *Donini, V. M., Lostorto, V., & Zamaro, N. (2022). Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente, 4 (2022): https://www.amministrativamente.com/index.php/formez/article/view/13339*

F. **Una ricompensa monetaria non è considerata un incentivo significativo** (solo il 3,8% donne, il 7,3% uomini).
G. **Lo studio ha sottolineato la necessità di un'ulteriore formazione** per aumentare la consapevolezza, promuovere il *whistleblowing* come dovere etico e migliorare le protezioni per creare fiducia nel sistema.

Inoltre, sempre con riferimento all'**Italia**, è interessante notare che l'ANAC, l'Autorità Nazionale Anticorruzione, ha sottoposto un questionario agli enti del settore pubblico e privato volto a verificare le soluzioni adottate in una fase di prima applicazione della normativa. **Nel settore pubblico, il 62% degli enti ha predisposto una piattaforma informatica specificatamente dedicata all'acquisizione e alla gestione delle segnalazioni in forma scritta**. Il 38% non ha predisposto una piattaforma e ha adottato diverse modalità di ricezione delle segnalazioni, come la posta elettronica certificata o la posta ordinaria.

A tal proposito si evidenziano due aspetti critici:

A. **Tra i soggetti che non hanno adottato la piattaforma ci sono anche le grandi amministrazioni**, che avrebbero tutti gli strumenti, in termini di disponibilità di risorse umane e materiali, per realizzare più facilmente l'infrastruttura informatica.
B. **La posta elettronica certificata e la posta ordinaria non costituiscono modalità adeguate** di ricezione delle segnalazioni, se non coadiuvate da specifiche contromisure volte a mitigare il rischio di comunicazione impropria dei dati.

Gli stessi profili di criticità evidenziati sopra sono stati riscontrati anche **nel settore privato: solo il 56% dei soggetti, infatti, ha attivato la piattaforma informatica** e circa il 64% ha dichiarato di aver previsto la possibilità di effettuare segnalazioni orali. Inoltre, è interessante notare che, nel settore privato, solo il 30% degli enti ha dichiarato di aver ricevuto segnalazioni di *whistleblowing*: questo è un segno che il quadro del *whistleblowing* è ancora poco conosciuto e deve essere ulteriormente incentivato.

Sia gli studi polacchi che quelli italiani rivelano che, **pur riconoscendo l'importanza del *whistleblowing*, lə dipendenti spesso non hanno fiducia nell'efficacia dei meccanismi di segnalazione e temono ritorsioni.** Mentre le iniziative di formazione, come si vede nello studio italiano, aiutano a migliorare la consapevolezza, le barriere culturali e le debolezze istituzionali continuano a ostacolare l'affermazione di solide culture del *whistleblowing*. Per affrontare queste sfide sono necessari non solo quadri giuridici, ma anche politiche organizzative proattive, una comunicazione più chiara e tutele rafforzate per promuovere una cultura dell'integrità e della trasparenza. Sebbene i risultati dell'indagine non siano rappresentativi e non possano essere generalizzati a livello nazionale, possono essere utili per imprenditori, *manager*, professionistə delle risorse umane e responsabili della *compliance*, che sono tutti *stakeholder* chiave responsabili dell'implementazione di sistemi di *whistleblowing* efficaci sul posto di lavoro.

5.2 INDICE PER LA VALUTAZIONE DELLA PROTEZIONE DELLE PERSONE SEGNALANTI (IEWP)

Alcunə ricercatorə hanno sviluppato il cosiddetto ***Index for Evaluating Whistleblower Protection*** **(IEWP**, letteralmente Indice per la valutazione della protezione dellə segnalanti): uno strumento digitale **per valutare l' efficacia dei meccanismi di protezione** in diversi Paesi e periodi di tempo.

L'IEWP è costituito da sotto-indici, sia quantitativi che qualitativi. A livello quantitativo, si valutano le garanzie istituzionali attraverso voci quali la sicurezza del lavoro, la riservatezza, la protezione dalle ritorsioni, l'immunità legale, i tassi di protezione dellə segnalanti, il numero di richieste di protezione rispetto alle segnalazioni di corruzione, ecc. A livello qualitativo, ci si concentra sull'acquisizione di percezioni ed esperienze relative al *whistleblowing*, comprese le percezioni di vari gruppi (funzionarə, espertə, cittadinə senza esperienza di *whistleblowing* e segnalanti stessə) ed esperienze dirette (di solə segnalanti).

L'IEWP consente di confrontare i livelli di protezione tra i vari Paesi e tiene anche traccia delle modifiche nel tempo. Oltre alla misurazione, evidenzia le principali aree di miglioramento, come l'attuazione tempestiva delle leggi, l'imparzialità nella nomina dellə funzionarə e la trasparenza nella disponibilità dei dati.

Lə autorə sostengono una metodologia a due pilastri, che combina i dati amministrativi con le risposte ai sondaggi, e sottolineano la necessità di standardizzare e migliorare l'accesso ai dati pertinenti.

5.2.1 L'esperienza di Transparency International

A seguito della pubblicazione di una metodologia per valutare la conformità dei progetti di legge nazionali con la Direttiva europea e le migliori pratiche implementate, *Transparency International* ha **sviluppato un quadro di autovalutazione per aiutare le organizzazioni a creare, implementare e rivedere i sistemi interni di *whistleblowing***, noto con l'acronimo **IWS (*Internal Whistleblowing System*,** appunto). L'IWS consente di verificare che i sistemi adottati siano efficaci, in linea con le migliori pratiche e gli standard internazionali. Il quadro comprende 130 domande suddivise in otto aree principali, che coprono vari aspetti, tra cui l'ambito di applicazione del sistema, la protezione offerta, la comunicazione interna ed esterna e il monitoraggio dell'efficacia. Le domande sono progettate per identificare i fattori che potrebbero compromettere l'efficacia del sistema e fornire alle organizzazioni una guida utile per migliorare il loro sistema di *whistleblowing*. Le risposte e i risultati ottenuti possono aiutare le organizzazioni a ottimizzare i loro sistemi.

5.3 INDICATORI CHIAVE PER LA VALUTAZIONE DEI SISTEMI DI WHISTLEBLOWING

Basandosi sugli strumenti e sui mezzi esistenti e tenendo conto dello stato e delle esigenze dei sistemi di protezione dellə segnalanti all'interno dell'UE e dei suoi Stati membri, le pagine del capitolo di questa guida mirano a **suggerire una serie di indicatori quantitativi e qualitativi** che possono essere utilizzati per valutare l'efficacia dei meccanismi di segnalazione delle irregolarità.

Sul fronte quantitativo, i principali indicatori di valutazione riguardano sostanzialmente il funzionamento dei meccanismi di segnalazione e i numeri corrispondenti. Dovrebbero sempre includere:

A. **Segnalazioni ricevute e segnalazioni motivate:** il numero totale di segnalazioni ricevute e la percentuale di quelle comprovate a seguito di indagini in un determinato periodo di tempo (per esempio, annualmente).
B. **Ispezioni e loro esiti**: il numero di ispezioni effettuate e i loro risultati.
C. **Tempi di risposta/risoluzione:** il tempo medio impiegato per confermare, indagare e risolvere i problemi relativi alle segnalazioni di *whistleblowing*.
D. **Accessibilità dei canali di segnalazione:** la disponibilità di canali basati sul genere, diversificati e di facile utilizzo (per esempio, moduli *online*, *hotline*, possibili incontri faccia a faccia), la loro fruibilità tra diversi gruppi demografici e il rispetto della parità di genere.
E. **Procedimenti giudiziari e sentenze:** il numero di procedimenti giudiziari avviati, compresi i procedimenti per porre fine alle azioni di ritorsione, e le sentenze emesse in un determinato periodo di tempo (per esempio, annualmente).
F. **Episodi di ritorsione e misure di protezione:** il numero di segnalanti che hanno subito ritorsioni e le misure adottate per affrontare tali casi (efficacia della protezione).
G. **Anonimato:** l'esistenza di procedure in grado di farsi carico di segnalazioni anonime circostanziate, oltre a quelle riservate.
H. **Azioni di *follow-up*:** la percentuale di casi che comportano azioni correttive, azioni organizzative o modifiche delle politiche interne all'ente.
I. **Sanzioni pecuniarie e/o recuperi:** importi riscossi a titolo di ammende e altre sanzioni pecuniarie imposte.
J. **Valutazione del danno patrimoniale:** valutazione delle perdite finanziarie legate a comportamenti scorretti segnalati.

Gli indicatori individuati forniscono informazioni misurabili sulle prestazioni del sistema. **I metodi di raccolta dei dati** per questi indicatori possono includere:

A. **Sondaggi e questionari** distribuiti a dipendenti e *stakeholder* per misurare la consapevolezza, la fiducia e la percezione dei sistemi di segnalazione.

B. **Analisi delle statistiche** dei rapporti, dei tassi di risoluzione e degli esiti della protezione, delle statistiche dei tribunali e delle relative metriche (analisi dei dati).
C. **Valutazione della conformità alla legislazione e alle linee guida** in materia di *whistleblowing*, alle regole interne e alle politiche (*audit* di conformità).

In Paesi come la **Bulgaria**, dove misurare l'efficacia del sistema di *whistleblowing* è difficile a causa del basso numero di segnalazioni e di procedimenti giudiziari (ma vale anche per l'**Italia**), l'attenzione dovrebbe focalizzarsi (anche e non solo, nel caso italiano) verso la creazione di fiducia attraverso esperienze positive e trasparenza. Un'azione rapida a seguito di una segnalazione e la garanzia della riservatezza sono fondamentali per **creare fiducia nel sistema** e incoraggiare un maggior numero di dipendenti a utilizzarlo. Se lə dipendenti vedono che le segnalazioni portano a risultati reali e che l'identità dellə segnalanti è mantenuta riservata, sarebbero più motivatə a partecipare.

Sul fronte qualitativo, l'accento dovrebbe essere posto su approcci indiretti o anonimizzati, come sondaggi aggregati, ricerche documentali o canali di *feedback* sicuri che garantiscano la riservatezza e la protezione dellə segnalanti. Questi includono:

A. ***Focus group*** condotti separatamente con dipendenti e segnalanti per esplorare le esperienze con il sistema e gli atteggiamenti culturali nei confronti della segnalazione.
B. **Casi studio** su:
    I. Analisi del quadro di protezione dei segnalanti, compresa la conformità alla Direttiva europea, alla legislazione nazionale, alle norme e alle procedure interne (conformità legale), nonché la disponibilità di supporto psicologico, assistenza legale e altre misure per i segnalanti (come i centri di supporto).
    II. Analisi di segnalazioni specifiche per valutare la gestione dei processi e i risultati.
    III. Analisi dei proventi finanziari di multe e sanzioni e valutazione dei danni patrimoniali identificati.
C. **Interviste alle parti interessate con attori esterni**, come organizzazioni della società civile, associazioni professionali, sindacati e autorità di regolamentazione, per esplorare la collaborazione e l'impatto sistemico.

Per incentivare il *whistleblowing* e migliorare i sistemi di segnalazione, possono essere raccomandati **strumenti aggiuntivi**, come ad esempio:

A. Pubblicazione di valutazioni dettagliate delle prestazioni dei sistemi di *whistleblowing* e sulla cultura della segnalazione.
B. Raccolta di *feedback* regolari da parte di segnalanti, dipendenti e parti interessate per identificare le lacune.
C. Utilizzare i risultati della valutazione per perfezionare i meccanismi di rendicontazione, i programmi di formazione e i quadri di protezione.

5.4 VALUTARE LA CULTURA DELLA VOCE

Una solida cultura della segnalazione (internazionalmente, *speak-up culture*) è essenziale per il successo dei sistemi di *whistleblowing*.

Per poterla rilevare, sono utili i metodi atti a valutare la fiducia dellə dipendenti nei canali di segnalazione, la loro disponibilità a segnalare le violazioni e la loro percezione della reattività del livello dirigenziale, pubblico o privato. A vari livelli dell'Unione europea, certamente la riservatezza, ossia la protezione dell'identità dellə segnalanti, è riconosciuta come precondizione fondamentale ed efficace per incoraggiare lə dipendenti a segnalare[75].

Per valutare l'ingaggio nella diffusione della cultura della segnalazione è possibile utilizzare una serie di strumenti che valutano la consapevolezza dellə dipendenti, la loro fiducia nel sistema di protezione dalle segnalazioni, la frequenza delle segnalazioni. In dettaglio, è possibile:

A. **Registrare la percentuale di dipendenti che sono a conoscenza dei meccanismi** di segnalazione e dei loro diritti in qualità di segnalanti, al fine di valutare la consapevolezza dellə dipendenti.
B. **Effettuare sondaggi per misurare la fiducia dellə dipendenti** nella risposta dell'organizzazione alle segnalazioni dellə segnalanti.
C. **Registrare la disponibilità e la capacità concreta di segnalazione** per come dichiarate dallə dipendenti o altri *stakeholder*.

Strumenti come sondaggi e *focus group* possono essere utilizzati anche per identificare gli ostacoli alla presentazione delle dichiarazioni e per supportare le strategie per creare un ambiente aperto e di supporto per lə segnalanti:

A. Sondaggi o interviste con lə dirigenti/manager sulla loro percezione del *whistleblowing* e sull'apertura delle segnalazioni possono fornire informazioni sugli atteggiamenti del *management/leadership*.
B. La fiducia degli *stakeholder* esterni nell'impegno dell'organizzazione per la protezione dellə segnalanti è una misura della fiducia del pubblico.
C. Il *feedback* dellə segnalanti sull'equità e la trasparenza delle indagini è un indicatore importante del livello di soddisfazione per la risoluzione dei problemi di *whistleblowing*.

In special modo **in Italia** (tramite le interviste condotte ai fini di questa guida) emerge come sia fondamentale la **sensibilizzazione dell'opinione pubblica**, rivelando spunti interessanti su questo tema ed evidenziando come occorra lavorare al fine di diffondere il *whistleblowing* tramite mezzi in grado di **raggiungere un pubblico più ampio possibile: eventi sportivi, festival, grandi eventi**. In concreto, si suggerisce che le stesse leghe

[75] *Garante europeo della protezione dei dati (GEPD). Linee guida sul trattamento delle informazioni personali nell'ambito di una procedura di whistleblowing, dicembre 2019: Si veda: https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf?utm_source=chatgpt.com*

calcistiche possano utilizzare l'impatto sulle grandi folle domenicali per lanciare una campagna di sensibilizzazione e farsi portavoce di un tema così delicato, come è stato fatto su altri temi come la discriminazione, l'abuso, il femminicidio.

Un altro suggerimento è quello di **sviluppare anche elementi e prassi di comunicazione attorno al *whistleblowing***, per valutarne la sua percezione pubblica e al tempo stesso favorirne la diffusione, tramite il giornalismo di comunità o il cosiddetto **giornalismo delle soluzioni.**

Secondo altrə, il *whistleblowing* rappresenta una **fondamentale libertà democratica**, da tutelare al pari della libertà di espressione, in quanto manifestazione stessa della democrazia. In questa prospettiva, il concetto di *whistleblowing* assume una valenza innovativa, **andando oltre il tradizionale ambito della *compliance*.**

Viene proposto anche un approccio interessante per contrastare la cultura del silenzio e stabilire una nuova etica: **aumentare la responsabilità della cittadinanza tutta**, diffondendo la consapevolezza che la segnalazione di irregolarità è una scelta personale, rafforzando quindi la **lettura dellə segnalante come una persona comune che fa una cosa ordinaria.**

Infine, è stato evidenziato il bisogno di **promuovere una cultura che renda il sistema** meno istituzionalizzato **e più orientato alla responsabilizzazione** anche individuale. Ciò minimizzerebbe il rischio di deresponsabilizzazione e di utilizzo non opportuno dell'istituto, riducendo quindi segnalazioni infondate e/o calunniose di norma mosse da interessi personali, le quali compromettono l'efficacia e l'affidabilità dei sistemi di segnalazione.

In Spagna, le interviste realizzate per questo progetto rivelano quanto occorra ancora **cambiare la cultura e la mentalità diffusa**, **promuovendo una lettura dellə segnalanti come "collaboratorə di integrità", una fonte intelligente di informazioni.** Al tempo stesso, occorrerebbe riuscire a dimostrare pubblicamente, *in primis* allə potenziali segnalanti, che l'istituto non è inutile, ma in grado di generare impatto positivo.

Ciò perché in **Spagna** è ancora forte una diffusa cultura del silenzio, guidata dalla paura di ritorsioni e dall'esclusione dal gruppo, che si può vedere sul posto di lavoro in modo simile allə bambini a scuola, dove chiunque segnali comportamenti inappropriati è visto tuttora come una spia.

Anche **in Bulgaria,** è emerso come la **cultura del *whistleblowing* sia ancora poco sviluppata,** e che il personale di un ente privato o pubblico abbia tuttora **scarso interesse o fiducia nell'utilizzo del sistema.** Lə intervistati hanno condiviso la consapevolezza che una cultura del *whistleblowing* fiduciosa deve essere sostenuta da una valutazione regolare e continuativa dell'efficacia del sistema, che generi un processo non episodico di monitoraggio e di adeguamento delle procedure in base ai

risultati della valutazione stessa. I suggerimenti includono l'esecuzione di revisioni periodiche delle politiche interne e la condivisione di esperienze tra organizzazioni diverse.

In particolar modo secondo lə avvocatə intervistatə, **è necessario stabilire un chiaro legame,** sia legislativo che pratico, nonché nella comprensione pubblica, **tra la protezione della libertà di parola nei casi SLAPP** (*Strategic Lawsuits Against Public Participation*) **e la protezione dellə segnalanti** (cfr. capitolo 4.1). Finora tale comprensione non è visibile nel diritto dell'UE, nel diritto nazionale, nella prassi giuridica e nella comprensione pubblica. Gli operatori del diritto stanno cercando di incorporare aspetti del concetto SLAPP e della legislazione sulla protezione dellə segnalanti nella difesa nei casi di diffamazione. Sebbene alcune giurisdizioni abbiano mostrato interesse per questo approccio, i risultati rimangono incerti a causa dell'assenza di una giurisprudenza consolidata. Si prevede tuttavia che alcuni degli esiti di questi casi diventeranno più chiari nel prossimo futuro.

5.5 VALUTAZIONE DEL COINVOLGIMENTO E DELLA COLLABORAZIONE DEGLI STAKEHOLDER

Gli *stakeholder* svolgono un ruolo fondamentale per il successo delle iniziative di *whistleblowing*, dal supporto alle politiche all'azione sui problemi segnalati. È quindi importante utilizzare metodi appropriati per valutare l'efficacia della collaborazione tra le parti interessate, concentrandosi sulla comunicazione, sull'allineamento delle politiche di *whistleblowing* e sugli sforzi congiunti di sensibilizzazione. **Una serie di indicatori può essere utilizzata per misurare la collaborazione tra le parti interessate.**

Gli indicatori suggeriti possono misurare:

A. **Frequenza dell'impegno**: numero di sessioni di formazione congiunte, campagne di sensibilizzazione o *forum* con altri *stakeholder*.
B. **Risorse condivise**: esistenza e utilizzo di partenariati per le risorse condivise (per esempio, patrocinio a spese dello Stato, strumenti di indagine).
C. **Sviluppo collaborativo delle politiche**: coinvolgimento delle parti interessate nello sviluppo di politiche o linee guida per lə segnalanti.

È possibile utilizzare una serie di **metodi per valutare il coinvolgimento e la collaborazione** degli *stakeholder* nelle iniziative di *whistleblowing*, tra cui:

A. **Sondaggi collaborativi** per valutare la soddisfazione degli *stakeholder* nei confronti delle iniziative congiunte, fornendo approfondimenti sulle loro percezioni di efficacia e sulle aree di miglioramento.
B. **Analisi della rete** per mappare il flusso di informazioni e risorse tra gli *stakeholder* e identificare i punti di forza e le lacune nella comunicazione e nella condivisione delle risorse.
C. **Analisi dei risultati** per misurare l'impatto tangibile degli sforzi di collaborazione, come l'aumento delle segnalazioni di irregolarità o dei

casi risolti.

FOCUS GOVERNO APERTO

La raccolta e l'analisi regolari dei dati sulle attività di *whistleblowing* sono fondamentali per valutare l'efficienza del sistema. Indicatori come quelli menzionati nel presente capitolo dovrebbero in ultima analisi orientare l'adeguamento delle politiche. I principi di governo aperto suggeriscono che:

A. I dati (ovviamente non quelli sensibili, ma quelli relativi alla valutazione) dovrebbero sempre essere pubblicati secondo **gli standard *Open Data* (dati aperti)**, al fine di permettere l'utilizzo e il riutilizzo delle analisi svolte.
B. Anche **le metodologie di analisi e valutazione dovrebbero essere sempre rese disponibili con licenza aperta**, al fine di favorire il miglioramento continuo dei metodi stessi e di promuovere la creazione di **comunità epistemiche, nazionali e internazionali**, composte da istituzioni e società civile, interessate a valutare il *whistleblowing* e il suo impatto. Pertanto, alla trasparenza dei dati dovrebbe sempre corrispondere la pubblicazione di informazioni sulle procedure di raccolta e sui processi di coinvolgimento delle parti interessate.
C. I risultati delle valutazioni, comunicati in modo trasparente e discussi tra le parti interessate, dovrebbero far sì che **le intuizioni portino a miglioramenti da ideare e attuare concretamente in ambiente di governo aperto**. Ciò può essere previsto sia nell'ambito di uno specifico impegno inserito nel Piano d'Azione Nazionale per il governo aperto (NAP), sia come una sfida autonoma (internazionalmente, *Open Government Challenge*, ossia impegni di riforma ambiziosi strutturati al di fuori del ciclo del Piano d'Azione Nazionale).
D. **Ai fini della valutazione d'impatto dell'utilità dei Centri di formazione, occorrerebbe valutare anche l'utilità di queste forme di supporto e il cambiamento che esse riescono a generare** nella percezione di chi segnala, così come dell'ambiente lavorativo corrispondente.

In sintesi, per migliorare e rendere più trasparenti le valutazioni periodiche dell'efficacia dei sistemi di *whistleblowing*, della cultura della segnalazione e del coinvolgimento degli *stakeholder*, si raccomandano i seguenti requisiti minimi:

A. **Pubblicazione periodica, almeno annuale, di valutazioni dettagliate sull'efficacia** del sistema di *whistleblowing* e sulla cultura del whistleblowing.
B. **Raccolta regolare di *feedback*** da parte di segnalanti, dipendenti e *stakeholder* per identificare lacune e aree di miglioramento.
C. **Utilizzo dei risultati della valutazione per perfezionare** i meccanismi di rendicontazione, i programmi di formazione e i quadri di protezione.

In conclusione: questa guida, incoraggiando la creazione delle infrastrutture necessarie per l'efficace attuazione del *whistleblowing*, al tempo stesso insiste con forza affinché **la valutazione non venga relegata a un ruolo marginale o considerata come ultima ruota del carro**. Al contrario, essa

deve essere formalmente affidata sia alle Autorità competenti sia a una comunità epistemica mista (istituzioni e società civile) ispirata al principio del governo aperto. La valutazione, infatti, è essenziale per il miglioramento del sistema e, più in generale, per la promozione della stessa cultura dell'integrità che ne è alla base.

FOCUS GENERE

La raccolta e l'analisi regolari dei dati sulle attività di *whistleblowing* sono fondamentali per valutare l'efficienza del sistema. Sebbene le donne tendano a condannare i comportamenti corrotti più degli uomini, **sembrano denunciare la corruzione meno spesso degli uomini**, come confermato dai dati del *Global Corruption Barometer* (GCB) di *Transparency International*[76].

Alcuni **risultati chiave** di diverse ricerche:

A. • Solo **il 48% delle donne ritiene di poter denunciare atti di corruzione senza il rischio di** ritorsioni, rispetto al 54% degli uomini[77].

B. • Incentivi alla rendicontazione: un'indagine sperimentale su oltre 2.000[78] dipendenti ha evidenziato come le **donne siano più incentivate degli uomini ad agire se ci sono tutele anti-ritorsione e obblighi di legge.**

C. • Secondo uno studio condotto in Italia[79], non vi è alcuna differenza significativa nella disponibilità a segnalare tra uomini e donne. Ciò che deve essere ulteriormente esplorato, tuttavia, è la **paura di ritorsioni da parte di *manager* e colleghi e l'aumento dello stress che le donne sperimentano** dopo la denuncia o segnalazione.

Nel complesso, sembra che tra i soggetti intervistati per questa guida, ci sia una **tendenza a non considerare le difficoltà e le complessità del "parlare" per le donne, ma più in generale per qualsiasi gruppo emarginato.** Tuttavia, se i dati mostrano che le donne tendono a parlare meno e a soffrire di più per la paura di ritorsioni, questo dovrebbe servire come indicatore dell'efficacia del sistema.

Si consiglia di:

A. **Tematizzare la questione delle donne che subiscono più danni** e ritorsioni rispetto agli uomini.

B. **Aumentare la consapevolezza di un approccio inclusivo** a tutte le diversità e ai gruppi più deboli che possono essere presenti in una cultura organizzativa.

C. **Sensibilizzare l'opinione pubblica sui casi** di *sextortion* e molestie sessuali (cfr. **capitolo 1** in approfondimento di genere)

D. **Pubblicazione di dati disaggregati per genere**, se disponibili: solo un numero limitato di organizzazioni include dati sul genere e sui fattori intersezionali. Questa lacuna rappresenta un'opportunità mancata per raccogliere informazioni aggiornate che potrebbero supportare un processo decisionale basato su dati concreti. Per affrontare questo problema, è essenziale rafforzare i meccanismi di raccolta e analisi dei dati, garantendo una comprensione più accurata del comportamento, delle esigenze e delle priorità delle persone segnalanti.

E. **Formazione e sensibilizzazione sul *whistleblowing* sensibile al genere.**

F. **Sviluppare un programma di formazione all'interno dell'organizzazione come**

Cp. 1 >

[76] *Si veda: Barometro globale della corruzione 2021 di Transparency International*

[77] *Si veda: Barometro globale della corruzione 2021 di Transparency International*

[78] *Si veda: https://knowledgehub.transparency.org/assets/uploads/helpdesk/Gender-sensitivity-in-corruption-reporting-and-whistleblowing_2020_PR.pdf*

[79] *Donini, V. M., Lostorto, V., & Zamaro, N. (2022). Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente, 4 (2022): https://www.amministrativamente.com/index.php/formez/article/view/13339*

misura preventiva, volto a educare tutti i membri e lə partecipanti alle pratiche di *whistleblowing*, con particolare attenzione al genere e all'intersezione di altri fattori di vulnerabilità, come la povertà e gli squilibri di potere. Il programma dovrebbe affrontare la segnalazione di molestie, abusi sessuali e comportamenti scorretti connessi alla corruzione, evidenziando nel contempo i diversi impatti su donne e uomini, in particolare l'onere sproporzionato per le donne. Occorre inoltre porre l'accento sulla prevenzione delle ritorsioni, come le molestie sessuali o la *sextortion*, e sulla sensibilizzazione in merito agli stereotipi di genere, ai pregiudizi e alle vulnerabilità specifiche che incidono sui segnalanti in situazioni di emarginazione.

G. **Definire un MEL (monitoraggio, valutazione e apprendimento) delle pratiche di *whistleblowing* sensibili al genere:**
   I. Implementare *audit* regolari per garantire che i sistemi di segnalazione garantiscano realmente la riservatezza, l'anonimato e la protezione dalle ritorsioni, in particolare nei casi basati sul genere.
   II. Condurre valutazioni d'impatto sensibili al genere per valutare se le protezioni dei segnalanti supportano efficacemente le donne, le persone LGBTQ+ e altri gruppi vulnerabili.
   III. Stabilire un meccanismo di feedback in cui lə segnalanti possano segnalare in modo anonimo problemi con il sistema, garantendo un miglioramento continuo.

Queste misure aiuteranno a valutare l'efficacia delle protezioni sensibili alla dimensione di genere all'interno del sistema di *whistleblowing*, garantendo che il sistema sia in continua evoluzione per proteggere meglio tuttə lə segnalanti, in particolare quellə che segnalano comportamenti scorretti basati sul genere.

5.6. RACCOMANDAZIONI

Cosa si può raccomandare sulla base degli studi empirici?

1. VALUTAZIONE CONTINUA

La valutazione deve divenire strutturale e non episodica, in quanto verifica puntuale del funzionamento del sistema.

2. MONITORAGGIO PERIODICO E COMPARATO

Tenendo conto dello studio empirico condotto in **Polonia** e **Italia** (2.3), si può raccomandare che **studi analoghi siano condotti periodicamente in tutti gli Stati membri** al fine di raccogliere dati pertinenti e sviluppare conoscenze teoriche ed empiriche sulla percezione e l'efficacia dei sistemi di *whistleblowing* in diversi contesti organizzativi e nazionali. Ciò consentirebbe di monitorare l'evoluzione dei sistemi e di migliorarne costantemente l'efficacia.

3. ADOZIONE DELL'INDICE IEWP

L'indice per la valutazione della protezione dellə segnalanti (IEWP) (2.4) può essere preso in considerazione e adattato dagli Stati membri quando sviluppano i propri indicatori di valutazione. Sebbene la IEWP si basi sulla ricerca del settore pubblico, può essere adattata per tracciare e valutare le segnalazioni di irregolarità nel settore privato e senza scopo di lucro,

coprendo così efficacemente tutte le forme di corruzione e le negligenze istituzionali.

4. RACCOMANDAZIONI DI TRASPARENCY INTERNATIONAL

Nell'istituire e mantenere un sistema interno di *whistleblowing*, è **necessario tenere conto di alcune raccomandazioni chiave di TI (2.5)**. Tra queste, la garanzia che il sistema sia conforme ai requisiti giuridici nazionali (leggi sulla protezione dellə segnalanti e altre leggi pertinenti come la protezione dei dati o il diritto del lavoro), che sia inclusivo e sensibile alla dimensione di genere, che sia formalmente riesaminato almeno una volta all'anno e che siano apportate le modifiche appropriate per migliorarne l'efficacia.

5. VALUTAZIONE MULTILIVELLO E PARTECIPATA

La valutazione deve essere formalmente affidata sia alle Autorità competenti sia a una comunità epistemica mista (istituzioni e società civile) ispirata al principio del governo aperto.

6. VALUTAZIONE D'IMPATTO DEI SERVIZI DI SUPPORTO

In chiave di valutazione d'impatto, si dovrebbe verificare l'**efficacia di servizi di supporto**, come i centri civici di informazione, rispetto alla fiducia di chi segnala e dell'ambiente circostante

6. RACCOMANDAZIONI SU GENERE E GOVERNO APERTO

Capitolo 6

6.1 FOCUS DI GENERE

Chiediamo un'efficace attuazione di politiche pubbliche di protezione dellə segnalanti che integrino canali sensibili al genere sia a livello organizzativo che esterno. È essenziale colmare le lacune delle normative esistenti, come la Direttiva europea sulla protezione dellə segnalanti e il quadro giuridico nazionale esistente, che non considerano esplicitamente gli aspetti legati al genere.

In questo senso:

A. I quadri normativi internazionali, nazionali e subnazionali dovrebbero rafforzare le misure volte a **stabilire meccanismi di protezione su misura** per le donne segnalanti e altri gruppi vulnerabili.
B. **Garantire che i canali di segnalazione siano accessibili, inclusivi e rispondenti** alle loro esigenze e ai loro rischi specifici.
C. Rafforzare i meccanismi di raccolta e analisi dei dati garantendo una **comprensione più accurata del comportamento, delle esigenze e delle priorità dellə segnalanti.**
D. L'attuazione di canali sensibili alla dimensione di genere e di politiche mirate migliorerebbe l'efficacia dei processi di sostegno, in particolare per le donne e altri gruppi vulnerabili. **Garantire che le procedure** per la segnalazione, l'indagine e la risoluzione dei reclami **siano attrezzate per gestire le disuguaglianze intersezionali.**
E. **Rafforzare le misure di sicurezza e riservatezza sensibili al genere nei sistemi di *whistleblowing*.** Garantire che i sistemi di segnalazione includano protezioni su misura per i comportamenti scorretti basati sul genere, salvaguardando l'anonimato dellə segnalanti e prevenendo ritorsioni, soprattutto in situazioni di squilibrio di potere.
F. **Implementare protocolli di riservatezza** per proteggere le segnalazioni basate sul genere, proteggendo le identità e prevenendo l'identificazione indiretta.
G. Sviluppare una **formazione e una sensibilizzazione sul *whistleblowing* sensibile al genere** come misura preventiva per educare tuttə lə partecipanti alle pratiche di *whistleblowing*, sul genere e sull'intersezione di altri fattori di vulnerabilità.

Il programma deve:

A. Affrontare la segnalazione di **molestie, abusi sessuali** e comportamenti scorretti legati alla corruzione.
B. Evidenziare i **diversi impatti sulle donne e sugli uomini**, in particolare l'onere sproporzionato che grava sulle donne.
C. Porre l'accento sulla **prevenzione delle ritorsioni,** come le molestie sessuali o la *sextortion*, e sulla sensibilizzazione sugli stereotipi di genere, sui pregiudizi e sulle vulnerabilità specifiche che hanno un impatto sui segnalanti in situazioni di emarginazione.

6.2 FOCUS SU GOVERNO APERTO

Chiediamo l'attuazione efficace di politiche di protezione dellə segnalanti che integrino principi di governo aperto come trasparenza, partecipazione, responsabilità e inclusione. È essenziale colmare le lacune nelle normative e nelle pratiche esistenti, in particolare laddove i sistemi di *whistleblowing* rimangono poco chiari, inaccessibili o scarsamente supportati sia dalle istituzioni che dalla società civile.

In tal senso:

A. I quadri internazionali, nazionali e subnazionali dovrebbero **rafforzare la collaborazione *multi-stakeholder*** per co-progettare e monitorare i sistemi di *whistleblowing*, combinando le prospettive istituzionali con le esperienze e le competenze delle organizzazioni della società civile (OSC), per garantire chiarezza, accessibilità e fiducia nel processo di segnalazione.
B. Gli *stakeholder* istituzionali e civici dovrebbero collaborare per garantire che i canali di segnalazione siano comprensibili, inclusivi e progettati pensando all'utente, utilizzando un **linguaggio semplice, esempi pratici e istruzioni chiare** durante tutto il percorso di segnalazione, comprese linee guida ripetute e moduli di facile utilizzo.
C. Rafforzare i meccanismi di **raccolta e analisi dei dati sulle pratiche di *whistleblowing*,** garantendo che i dati siano **pubblicati in formati aperti** e utilizzati per informare le politiche attraverso dialoghi trasparenti con le parti interessate e cicli iterativi di miglioramento.
D. **Implementare sistemi di formazione e supporto per lə funzionarə pubblicə e lə gestorə di segnalazioni interne**, andando oltre un approccio puramente legalistico per includere l'apprendimento esperienziale basato su dilemmi etici e simulazioni di casi reali, in collaborazione tra autorità pubbliche e OSC.
E. **Sviluppare campagne di comunicazione congiunte per sensibilizzare** l'opinione pubblica sui diritti dellə segnalanti e sui servizi di supporto disponibili, sfruttando i *media* nazionali, le piattaforme culturali e gli eventi sportivi per raggiungere un pubblico diversificato.
F. **Promuovere valutazioni partecipative dei rischi** per identificare potenziali aree di cattiva condotta rilevanti per il *whistleblowing* all'interno delle istituzioni, coinvolgendo sia gli attori interni che la società civile per garantire che i sistemi siano personalizzati e sensibili al contesto.

G. **Stabilire solide linee guida sulla protezione dei dati** sviluppate congiuntamente dalle autorità di protezione dei dati e dalle organizzazioni di supporto, garantendo che i servizi di consulenza possano trattare i dati personali in modo significativo ma sicuro, bilanciando la *privacy* con un supporto efficace.

H. **Co-progettare nuove leggi o regolamenti per espandere i meccanismi di protezione** in modo da includere non solo lə segnalanti ma anche coloro che li assistono, come le organizzazioni della società civile di supporto, lə consulenti legali e lə giornalistə, garantendo che siano protettə dalle ritorsioni, in linea con le migliori pratiche internazionali e i quadri normativi in materia di diritti umani.

Creare e mantenere registri pubblici dei centri di informazione civica e istituzionale, definendo chiari criteri di inclusione e valutandone il loro impatto, promuovendo il coordinamento tra le organizzazioni elencate per segnalare efficacemente lə segnalanti e monitorare le sfide sistemiche attraverso un regolare scambio tra pari.

OLTRE QUESTA GUIDA

Le pagine di questa guida hanno fatto emergere un aspetto cruciale: la Direttiva europea e le leggi nazionali di conversione hanno contribuito a migliorare il quadro normativo, ma altre riforme (alcune delle quali sono incluse nelle raccomandazioni alla fine dei capitoli precedenti) possono migliorare ulteriormente l'impatto atteso sulla buona *governance* auspicata.

Tale impegno politico “dall'alto verso il basso” in materia di *whistleblowing*, tuttavia, necessita di solide basi per produrre un impatto significativo sul complesso ambiente sociale e istituzionale in cui emergono continuamente opportunità di corruzione e altri illeciti. Queste basi sono fondate su valori, principi, aspettative, credenze: in altre parole, **la dimensione culturale è cruciale per potenziare norme informali e giudizi condivisi**, incoraggiando e sostenendo socialmente il *whistleblowing* come componente normale e preziosa di una cultura della segnalazione auspicabile. I tratti culturali che prevalgono all'interno di determinate organizzazioni o società, infatti, incidono in modo decisivo sull'efficacia di qualsiasi implementazione del *whistleblowing*. Soprattutto in ambienti in cui la corruzione e gli illeciti sono normalizzati come regole non scritte, la pressione sociale contro i soggetti segnalanti può essere l'atteggiamento dominante e di successo. **La cultura non può essere cambiata per decreto, ovviamente, ma le riforme della regolamentazione formale forniscono segnali che stimolano cambiamenti sociali**: possono avviare un processo lento, che nel tempo può generare profondi cambiamenti nel modo in cui gli individui percepiscono e giudicano i comportamenti propri e altrui.

Il paradossale dilemma dellə segnalante, ritratto alternativamente come eroə o traditorə, riflette proprio la resistenza a *normalizzare* la pratica di segnalare potenziali illeciti nell'interesse pubblico, rafforzando la connessione tra approcci *whistleblowing-oriented* e *whistleblower-oriented*, ovvero tra la dimensione formale e la prospettiva soggettiva e valoriale, per come fatto in queste pagine.

Per rendere efficace il *whistleblowing*, è necessario trovare un **attento equilibrio tra interessi, aspettative e diritti contrastanti dei diversi attori coinvolti nel processo.** Le sfide sostanziali associate a qualsiasi quadro normativo in materia di *whistleblowing* sono state chiaramente evidenziate nei capitoli precedenti. Come ridurre al minimo i rischi di ritorsioni, come salvaguardare i diritti alla *privacy* e proteggere i dati sensibili, come verificare il contenuto delle segnalazioni di *whistleblowing*, per esempio, sono questioni complesse.

Le innovazioni digitali presentano sia opportunità che sfide: le piattaforme *online* e gli strumenti di comunicazione sicuri possono facilitare la segnalazione anonima e migliorare la protezione, ma sollevano anche preoccupazioni in merito alla sicurezza dei dati e al potenziale uso improprio. **Bilanciare i vantaggi degli strumenti digitali con la necessità di proteggere le informazioni sensibili è una questione critica.** In altre

parole, non si può imporre una formula universale e adatta a chiunque e a qualunque contesto: la regolamentazione del *whistleblowing* dovrebbe consentire a qualsiasi organizzazione pubblica o privata, con le proprie caratteristiche e il proprio *background*, di personalizzare il proprio *mix* particolare e specifico di incentivi, vincoli, educazione, applicazione.

Il *whistleblowing* ha un enorme potenziale come strumento anticorruzione. La sua efficacia, tuttavia, dipende dall'affrontare queste sfide. Un'analisi empirica approfondita sui fondamenti morali e motivazionali della segnalazione dellə segnalanti sembra una fonte di conoscenza necessaria per migliorare l' **efficacia percepita** delle politiche corrispondenti. Inoltre, si dovrebbe approfondire il ruolo della formazione etica e degli strumenti educativi. Quest'ultima, infatti, dovrebbe essere efficace per aumentare la congruenza dei valori delle persone, nei quali essi vengono socializzati negli ambiti del riconoscimento sociale all'interno di organizzazioni pubbliche e private, con regole e procedure orientate all'interesse pubblico. Quando prevale un certo **stigma sociale** nei confronti del ruolo di chi segnala, anche le piattaforme più sofisticate per la segnalazione riservata o anonima saranno inutili. Una perseverante attività di "**formazione etica**" all'interno degli apparati pubblici, così come delle organizzazioni private, potrebbe assumere un **ruolo cruciale** in questo senso. Tale impegno dovrebbe essere finalizzato al rafforzamento dei circuiti sociali di riconoscimento reciproco e al **positivo rafforzamento** della lealtà verso gli obiettivi delle organizzazioni pubbliche e private, al consolidamento delle barriere morali contro la corruzione e delle motivazioni etiche alla base della segnalazione degli illeciti.

In conclusione, appare necessario **riconsiderare la dimensione sociale e comunitaria** all'interno della quale si vanno plasmando nel tempo le fonti di riconoscimento morale, che sono il principale motore della decisione di "soffiare nel fischietto". Del resto, il successo della regolamentazione e della legislazione sul *whistleblowing* dipende in primo luogo dal suo coordinamento all'interno di una più ampia azione collettiva anticorruzione "**dal basso**", che coinvolga tutti i più importanti ambiti sociali, da quello lavorativo a quello professionale, associativo, politico, sindacale, religioso. Solo in tali contesti, infatti, può generarsi il fermento per un **cambiamento culturale**, ovvero un quadro vincolante di credenze e norme informali in cui il *whistleblowing* sia incoraggiato e sostenuto reciprocamente attraverso l'espressione pubblica di giudizi etici positivi sui suoi effetti socialmente benefici.

ALLEGATO I: METODOLOGIA DI RICERCA E RACCOLTA DEI DATI

Questa guida pratica è il risultato dell'esperienza di ciascun partner nel settore e di una ricerca condotta con metodi misti da giugno 2024 a novembre 2024 in quattro fasi chiave:

1. Analisi dei documenti e ricerca bibliografica

In questa fase è stato stabilito un quadro concettuale e normativo della protezione dellə segnalanti, valutando gli obblighi, il livello di attuazione e le lacune.

2. Analisi e mappatura degli *stakeholder*

In questa fase, sono stati identificati e mappati cinquanta *stakeholder* tra organizzazioni della società civile (OSC), autorità, settore privato, mezzi di comunicazione, ordini professionali, mondo accademico e sindacati. Questi sono gli attori che potrebbero influenzare o sono importanti per promuovere la legislazione e la consapevolezza del *whistleblowing*. Il *database* degli *stakeholder* è stato la base per preparare un elenco di organizzazioni per la ricerca qualitativa e le interviste.

3. Interviste a espertə chiave

In questa fase sono statiə intervistatə lə rappresentanti di almeno cinque organizzazioni per Paese per raccogliere informazioni su sfide, opportunità, raccomandazioni e linee guida. La struttura delle interviste è stata costruita sulla base degli argomenti della guida, tuttavia il metodo utilizzato è quello di interviste semi-strutturate con espertə, per adattarsi alle risposte dellə intervistatə. Ciò è particolarmente utile per esplorare pratiche innovative che potrebbero non essere state prese in considerazione durante la progettazione. Ogni intervistatorə ha raccolto un consenso formale per rispettare pienamente la protezione dei dati. Sono state prodotte registrazioni audio.

4. Analisi

Le interviste sono state analizzate utilizzando un formato riassuntivo, che collega il contenuto dell'intervista a ciascun capitolo ed evidenzia i seguenti temi chiave:

A. Buone pratiche esistenti, implementate dall'organizzazione intervistata o citate da essa.
B. Bisogni e sfide identificate dall'intervistatə in relazione all'argomento del capitolo.
C. Proposte o punti chiave di azione per migliorare la situazione attuale.

Inoltre, i principali argomenti emersi dalle interviste, sono stati raccolti e riassunti, in maniera comparabile, in un file *excel*.

ALLEGATO II: ACRONIMI

ANAC: Autorità Nazionale Anticorruzione

CATI: Interviste telefoniche assistite da computer (*Computer-Assisted Telephone Interviewing*)

CAWI: Interviste Web assistite da computer (*Computer-Assisted Web Interviewing*)

CEDU: Convenzione europea dei diritti dell'uomo

CPDP: Commissione per la protezione dei dati personali (*Commission for Personal Data Protection*)

DPO: Responsabile della protezione dei dati (*Data Protection Officer*)

DSA: Legge sui servizi digitali *(Digital Services Act)*

GCB: Barometro globale della corruzione di Transparency International (*Global Corruption Barometer*)

GDPR: Regolamento generale sulla protezione dei dati (*General Data Protection Regulation*)

IEWP: Indice per la valutazione della protezione dellə segnalanti (*Index for Evaluating Whistleblower Protection)*

OCSE: Organizzazione per la cooperazione e lo sviluppo economico

OGP: Partenariato per il governo aperto (*Open Government Partnership*)

OMS: Organizzazione Mondiale della Sanità

ONG: Organizzazione Non Governativa

ONU: Organizzazione delle Nazioni Unite

OSC: Organizzazione della società civile

SLAPP: Cause strategiche contro la partecipazione pubblica *(Strategic Lawsuits Against Public Participation)*

SNA: Scuola Nazionale di Amministrazione

TFUE: Trattato sul funzionamento dell'Unione europea

UE: Unione Europea

UNODC: Ufficio delle Nazioni Unite contro la droga e il crimine *(United Nations Office on Drugs and Crime)*

WCAG: Linee guida per l'accessibilità dei contenuti web *(Web Content Accessibility Guidelines)*

W3C: Consorzio del World Wide Web (*World Wide Web Consortium*)

WMS: Sistemi di gestione delle segnalazioni *(Whistleblowing Management System)*

Open the whistle

GUIDA PRATICA AL WHISTLEBLOWING

OPWHI open the whistle

Cofinanziato dall'Unione europea