Nuove linee guida whistleblowing: modalità di gestione delle segnalazioni

Scritto da Interdata Cuzzola | 13/07/2021

Proseguendo nell'analisi della Delibera ANAC n. 469 del 9 giugno 2021, ci occupiamo della gestione delle segnalazioni che, come è noto, deve essere informatizzata, con il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante, del contenuto delle segnalazioni e della relativa documentazione.

L'amministrazione deve dare notizia dell'adozione del sistema applicativo informatico di gestione delle segnalazioni nella home page del proprio sito istituzionale in modo chiaro e visibile; tuttavia, anche al fine di evitare usi impropri del sistema, l'indirizzo web della piattaforma, sebbene raggiungibile da Internet, potrà non essere reso pubblico sul sito istituzionale dell'amministrazione. In tal caso, esso potrà essere reso noto ai soggetti interessati esterni all'amministrazione (lavoratori e collaboratori delle imprese che realizzano opere in favore della p.a.) per altre vie (ad es. mediante comunicazione diretta del link al momento della sottoscrizione del contratto).

L'amministrazione che non ha automatizzato il processo di gestione delle segnalazioni, a causa di specifiche difficoltà organizzative da motivare adeguatamente, può, in via residuale, utilizzare canali e tecniche tradizionali da disciplinare nel PTPCT o nell'atto organizzativo indicando, tuttavia, gli strumenti previsti per garantire la riservatezza dell'identità del segnalante, del contenuto delle segnalazioni e della relativa documentazione, in conformità a quanto previsto dalla legge. Ad esempio, può essere prevista la trasmissione cartacea della segnalazione in busta chiusa indirizzata al RPCT con la dicitura "riservata/personale".

Con riguardo alle segnalazioni pervenute mediante canali diversi dalla procedura informatica, si ritiene opportuno che queste siano protocollate in apposito registro riservato.

In generale, per il processo di gestione delle segnalazioni attraverso il supporto di una procedura informatica possono essere individuati i seguenti ruoli da assegnare agli utenti del sistema:

- segnalante: soggetto che ha inviato la segnalazione di whistleblowing;
- RPCT: Responsabile Prevenzione della Corruzione e Trasparenza nominato dall'ente, coinvolto nel trattamento dati personali presenti nella segnalazione;
- istruttore: fa parte della struttura di supporto del RPCT, è coinvolto nell'analisi della segnalazione e nella eventuale istruttoria; questo ruolo consente l'accesso a tutte le informazioni inserite nelle segnalazioni; è, altresì, coinvolto nel trattamento dati personali presenti nella segnalazione;
- custode delle identità: è il soggetto individuato dall'amministrazione che, su esplicita e motivata richiesta, consente al RPCT di accedere all'identità del segnalante. L'identità del segnalante non è nota al custode. Tale ruolo può anche coincidere con quello di RPCT. Non è coinvolto nel trattamento dati personali presenti nella segnalazione.

Nelle specifiche procedurali che seguono si fa riferimento a tali soggetti quali attori del processo o di

parte di esso.

Si precisa che l'amministrazione, nel trattamento delle segnalazioni attraverso una procedura informatica, deve attenersi alla normativa vigente sul trattamento dei dati personali, con particolare riguardo ai soggetti interni che sono coinvolti nel trattamento di tali dati.

Per tutelare il dipendente che segnala gli illeciti e garantire, quindi, l'efficacia del processo di segnalazione, la procedura di gestione delle segnalazioni utilizzata deve:

- consentire la gestione delle segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- presentare al segnalante l'informativa sul trattamento dei dati personali da parte dell'amministrazione ed eventualmente acquisire, già in fase di segnalazione, il consenso del

segnalante a rivelare l'identità all'ufficio di disciplina;

- identificare ogni segnalazione ricevuta mediante l'attribuzione di un codice univoco progressivo, registrando la data e l'ora di ricezione; tali informazioni dovranno essere associate stabilmente alla segnalazione;
- tutelare la riservatezza dell'identità del segnalante, del contenuto della segnalazione, della documentazione ad essa allegata nonché dell'identità di eventuali soggetti segnalati, garantendo l'accesso a tali informazioni solo ai soggetti autorizzati e previsti nell'iter procedurale;
- separare il contenuto della segnalazione dall'identità del segnalante;
- rendere disponibile il solo contenuto della segnalazione ai soggetti che gestiscono l'istruttoria;
- prevedere l'accesso sicuro e protetto all'applicazione per tutti gli utenti mediante l'adozione di sistemi di autenticazione e autorizzazione opportuni
- la piattaforma per l'acquisizione e gestione delle segnalazioni deve assicurare l'accesso selettivo ai dati delle segnalazioni, da parte dei diversi soggetti autorizzati al trattamento, prevedendo, ad esempio, una procedura per l'assegnazione, da parte del RPCT, della trattazione di specifiche segnalazioni all'eventuale personale di supporto;
- tracciare l'attività degli utenti del sistema nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. I relativi log devono essere adeguatamente protetti da accessi non autorizzati e devono essere conservati per un termine congruo rispetto alle finalità di tracciamento. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante. Il tracciamento può essere effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati;
- consentire l'accesso del RPCT all'identità del segnalante esclusivamente dietro espresso consenso del "custode" dell'identità dal segnalante;
- consentire nel corso dell'istruttoria lo scambio di messaggi o documenti tra segnalante e istruttore mediante meccanismi interni alla piattaforma che tutelino l'identità del segnalante. È esclusa l'adozione della posta elettronica individuale quale mezzo di notifica al segnalante;
- qualora la piattaforma per l'acquisizione e gestione delle segnalazioni invii messaggi (es. in caso di variazione dello stato di avanzamento dell'istruttoria, riscontro del segnalante a una richiesta di integrazione, riscontro del segnalante a una richiesta di consenso a rivelare la propria identità nell'ambito di un procedimento disciplinare, ecc.) sulla casella di posta elettronica individuale che l'amministrazione o l'ente ha assegnato al RPCT e all'istruttore, tali messaggi non devono contenere riferimenti all'identità del segnalante o all'oggetto della segnalazione;

- tutelare la riservatezza degli atti formati nel corso dell'attività istruttoria svolta dall'amministrazione;
- consentire al segnalante di verificare, in qualsiasi momento tramite l'applicazione, lo stato di avanzamento dell'istruttoria;
- consentire in qualsiasi momento, tramite l'applicazione, la fruibilità della documentazione custodita, ad es. al fine di evitare il download o, soprattutto, la stampa della stessa;
- rendere chiaramente visibili al segnalante, al fine di consentire l'uso consapevole e sicuro della piattaforma, le seguenti indicazioni da considerarsi requisiti minimi di buon comportamento, acquisendo dallo stesso segnalante la conferma di lettura:
    - *"È opportuno rimuovere riferimenti all'identità del segnalante dalla segnalazione e dai suoi allegati";*
    - *"Se per inviare la segnalazione è stato utilizzato il canale informatico è opportuno utilizzare il medesimo canale per tutte le comunicazioni successive da inviare all'Ente".*

Sempre al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte occorre altresì effettuare idonee scelte relativamente a modalità di conservazione dei dati (fisico, logico, ibrido); politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati); politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico); politiche di sicurezza (ad es. modifica periodica delle password); tempo di conservazione (durata di conservazione di dati e documenti).

Si raccomanda, inoltre, l'adozione di un idoneo modello organizzativo che definisca le responsabilità in tutte le fasi del processo di gestione delle segnalazioni, con particolare riguardo agli aspetti di sicurezza e di trattamento delle informazioni. Tali misure trovano specifica applicazione in relazione alle caratteristiche del sistema informatico realizzato e, tipicamente, si inseriscono nell'ambito dei presidi di sicurezza delle informazioni di carattere tecnico ed organizzativo predisposti dall'amministrazione nella gestione dei sistemi informativi.

Si rammenta che la mancata attivazione di procedure, ovvero l'adozione di procedure non conformi a quelle indicate nelle presenti Linee guida per l'inoltro e la gestione delle segnalazioni, è sanzionabile da parte dell'Autorità (art. 54-bis, co. 6, secondo periodo). Responsabile della mancata attivazione è considerato l'organo di indirizzo politico dell'amministrazione che ha adottato il PTPCT e nominato il RPCT. Resta fermo che l'amministrazione può stabilire ex ante altri responsabili nel PTPCT o in apposito atto organizzativo.