Alla Cortese Attenzione
Dell'Ufficio Regolazione e
Dell'Ufficio Whistleblowing

Milano, 9 settembre 2021

Transparency International Italia e Whistleblowing Solutions hanno avviato il progetto *WhistleblowingPA* a settembre 2018 per mettere a disposizione gratuitamente alle Pubbliche Amministrazioni una piattaforma informatica crittografata, come previsto dalla Legge n.179/2017. L'obiettivo era quello di fornire uno strumento sicuro e aggiornato, di semplice utilizzo e che non richiedesse sofisticate conoscenze informatiche da parte degli utilizzatori.

In considerazione della scarna normativa di riferimento, in questi anni non è sempre stato semplice allineare il servizio, ottemperando alle disposizioni fornite dal legislatore sia in materia di protezione dei dati personali che rispetto alle disposizioni di cui alla Legge citata. Siamo tuttavia riusciti a portare avanti il lavoro anche grazie ai colloqui con AGID e con il Garante per la Protezione dei Dati Personali.

Scriviamo ora ad A.N.AC. in seguito alla pubblicazione delle prime Linee Guida (di seguito anche LLGG) in materia di *whistleblowing* successive all'approvazione della Legge n.179/2017, la prima a prevedere un obbligo del canale della piattaforma informatica.

Al fine dell'adeguamento del nostro servizio alle Linee Guida, chiederemmo chiarimenti in merito ad alcune disposizioni. Chiediamo inoltre se sia prevista la pubblicazione di una guida operativa.

La figura del custode

Le Linee Guida hanno introdotto la figura del custode: avremmo bisogno di alcuni chiarimenti affinché l'implementazione da parte del nostro progetto sia conforme con le interpretazioni di A.N.AC.:

- La funzione del custode è obbligatoria per le piattaforme informatiche?
- Si può garantire al segnalante la possibilità di scegliere di rivelare al RPCT la propria identità, così da permettere a quest'ultimo un accertamento che tenga conto di chi sia la persona da tutelare?
- Ci sono indicazioni sui profili professionali più adeguati per rivestire tale qualifica?
- Quali sono le motivazioni che possono essere richieste al custode affinché venga sbloccata l'identità per il RPCT?
- Le LLGG indicano che il custode può anche coincidere con il RPCT: in tal caso, vi sarebbe una sovrapposizione tra i soggetti cui richiedere lo sblocco dei dati identificativi del segnalante. Sarebbe sufficiente che il sistema registri l'accesso all'identità da parte dell'RPCT?
- Il custode deve essere autorizzato al trattamento dei dati? Di fatto, anche se non ha accesso alle informazioni contenute nella segnalazione, le gestisce (alla stregua dei soggetti esterni all'ente che si occupano della manutenzione delle piattaforme stesse).
- Esistono dei requisiti specifici che la piattaforma deve prevedere per evitare che nei dati che finiscono nel cassetto del custode vengano inseriti dati falsi o non corretti (es. Mario o Maria Rossi)?

Pubblicazione della piattaforma

A.N.AC. indica che l'Amministrazione dà notizia dell'adozione del sistema applicativo informatico di gestione delle segnalazioni nella home page del proprio sito istituzionale in modo chiaro e visibile. Tale informativa deve essere trattata come una news (se si, quanto deve rimanere in homepage?) o di un contenuto permanente.

D'altra parte, viene indicato che "*l'indirizzo web della piattaforma, sebbene raggiungibile da Internet, potrà non essere reso pubblico sul sito istituzionale dell'amministrazione*". Sul punto necessiteremmo di chiarimenti, rispetto all'affermazioni di cui al passaggio precedente.

Si aggiunge che "*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)*". Tuttavia, la comunicazione dell'indirizzo della piattaforma attraverso questi altri canali preclude a moltissimi soggetti legittimati l'accesso ai canali di segnalazione stessa. Collaboratori e dipendenti delle società in controllo pubblico potrebbero non essere messi a conoscenza del canale o potrebbero entrare in servizio presso questi in un momento successivo alla sottoscrizione del contratto. In questo caso le Linee Guida parrebbero limitare un diritto previsto dalla legge: al proposito, avremmo necessità di ricevere specifiche sulla corretta interpretazione.

Del pari per il periodo che segue. A.N.AC. conclude infatti indicando che "*in assenza della pubblicazione sul proprio sito Internet, l'Amministrazione è comunque tenuta a garantire l'accesso non ristretto ai lavoratori e collaboratori delle imprese fornitrici che realizzano opere in favore dell'amministrazione pubblica, contemplati nel co. 2 del novellato art. 54-bis d.lgs. 165/2001*". Ci sembra però che una modalità che preveda che uno di questi soggetti debba fare una richiesta per conoscere le modalità di segnalazione, finisca con esporre gli stessi.

Chiediamo quindi quale sia l'interpretazione corretta, posto che ad oggi il nostro progetto richiede agli enti che la pubblicazione della piattaforma sia obbligatoria sul sito dell'ente, anche se non viene data indicazione della sezione più adeguata.

Gruppo di lavoro a supporto del RPCT

Le LLGG prevedono la possibilità per il RPCT di nominare figure di supporto per la gestione delle segnalazioni. Queste figure devono avere funzioni di accesso distinte rispetto al RPCT?

In che modo si configura la responsabilità di questi soggetti rispetto al RPCT, che è l'unico per il quale la legge prevede specifici compiti, responsabilità, nonché sanzioni?

Devono quindi essere registrati i diversi accessi? L'accesso può essere consentito anche in un secondo momento? L'accesso, nonché la conoscenza del testo stesso della segnalazione, può essere consentito solo a soggetti definiti in apposito atto organizzativo? Questi soggetti possono richiedere al custode accesso all'identità del segnalante?

Assegnazione

L'accesso o l'assegnazione di una segnalazione ad un ricevente deve essere mediato sempre e comunque dal RPCT di volta in volta, segnalazione per segnalazione, o può essere consentito automaticamente per ogni segnalazione ricevuta?

L'accesso deve essere revocabile e, se sì, chi deve avere la possibilità di revocarlo?

Ad un ricevente a cui sia stata assegnata la segnalazione deve essere consentito poterla riassegnare ad un collega/ufficio più appropriato o questa facoltà di assegnazione deve essere specificatamente disponibile al solo RPCT?

Per questa caratteristica di assegnazione, come per ogni altra indicazione fornita nelle LLGG, si chiede gentilmente di specificare il processo di gestione previsto e di esplicitare quali parti delle LLGG siano da implementarsi alla lettera e quali da interpretarsi come mera indicazione di massima non obbligatoria.

Accesso e continuità

Nel momento in cui ci sia un avvicendamento di RPCT, ci chiediamo se debba essere data continuità di accesso alle segnalazioni ricevute dal RPCT precedente anche al nuovo o se quest'ultimo debba avere accesso solo alle segnalazioni successive al suo incarico. Il nostro orientamento ci fa pensare alla continuità, per diversi motivi:

1. Nella gestione di segnalazioni di *whistleblowing* la protezione dei segnalanti è legata alla funzione stessa/incarico di RPCT.
2. Non è detto che, nel momento di un passaggio di consegne, la gestione di una o più segnalazioni sia conclusa ed è quindi opportuno che il nuovo RPCT abbia accesso alle segnalazioni.
3. In caso di nuove segnalazioni potrebbe essere utile per il nuovo RPCT conoscere se in passato siano state fatte segnalazioni su temi simili.
4. La legge non impone scadenze all'obbligo di riservatezza; quindi di fatto il nuovo RPCT eredita gli obblighi che erano a carico del RPCT precedente.

D'altro canto, riconosciamo che un segnalante potrebbe aver segnalato internamente al RPCT proprio perché la funzione era ricoperta da una certa persona e, possibilmente, non lo avrebbero fatto se la funzione fosse stata ricoperta dal nuovo RPCT (per possibili molteplici ragioni, come il collegamento di quest'ultimo con il soggetto segnalato o la scarsa fiducia nel soggetto). In questo caso si andrebbe a rompere il legame fiduciario tra segnalante e ricevente, perché il ricevente non corrisponderebbe più al soggetto a cui è stata inviata la segnalazione.

Tempo di conservazione delle segnalazioni

A.N.AC. indica in 5 anni il tempo di conservazione delle segnalazioni. Non ci è chiaro se si tratta di un termine massimo o minimo. Mantenere sulla piattaforma per 5 anni segnalazioni archiviate o non rilevanti ai fini della procedura di *whistleblowing* sembrerebbe in contrasto con i principi del GDPR che prevedono una minimizzazione nel trattamento dei dati. Ci si chiede quindi se questa indicazione sia perentoria e se riguardi

la conservazione di informazioni sulla piattaforma o la conservazione delle segnalazioni in generale da parte del RPCT anche su altri supporti.

Connessione e anonimizzazione

Le LLGG indicano che "per garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione" lo strumento debba utilizzare strumenti di anonimizzazione dei dati di navigazione implementando un accesso mediato dalla rete Tor. Chiediamo se vi siano alternative o effettivamente, stante la vostra analisi corrente, la tecnologia Tor sia la sola alternativa possibile atta a garantire anonimato in relazione ai metadati di rete.

Giovanni Colombo
Direttore Esecutivo Transparency International Italia

Giovanni Pellerano
Amministratore Delegato Whistleblowing Solutions