TRASPARENZA AMMINISTRATIVA

LEGGE 179/2017: Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarita' di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato

Sistema di Segnalazione di eventuali Illeciti riguardanti la Società Garda Uno SpA posto a disposizione di Dipendenti, Amministratori, Fornitori, Cittadini

1. Premessa

La Normativa che verte sull'emersione dei tentativi di corruzione nell'ambito Pubblico e Privato, ha visto una evoluzione significativa con l'approvazione della Legge 179/2017 modificativa dell'art. 54bis della Legge 165/2001.

La norma vede l'introduzione e la previsione di specifiche procedure atte a permettere ad un Segnalatore (qualsiasi sia la sua natura e posizione rispetto a quanto segnalato) di poter far emergere un illecito pur vedendo garantita la riservatezza della sua identità. Gli illeciti sono identificabili in: episodi Corruttivi, Concussivi, malversazione delle risorse pubbliche, incompatibilità di incarichi, Mobbing, discriminazioni sul luogo di lavoro, abuso d'ufficio, inquinamento dell'azione amministrativa *ab externo* e in generale, a titolo meramente esemplificativo, ai casi di sprechi, nepotismo, demansionamenti, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro.

L'Ente pubblico o anche la Società a controllo Pubblico di diritto Privato, ha pertanto l'obbligo di offrire al potenziale segnalante uno strumento atto allo scopo prefissato dalla Legge.

Le modalità di segnalazione possibili sono di diverso tipo e permettono, in funzione della modalità adottata dall'Ente o Società e ognuna offre un diverso grado di riservatezza con, di conseguenza, un

diverso gradimento al Segnalante riguardo alla difesa della sua identità. Possono essere riassunte come segue:

Strumento	Livello riservatezza	Possibile livello di gradimento
Informativa verbale al RPCT	bassa	scarso
Comunicazione scritta al RPCT	bassa	scarso
Comunicazione a mezzo email privata al RPCT	medio/bassa	medio/scarso
Comunicazione a mezzo sistema informatico su rete pubblica (internet)	media	medio/alto
Comunicazione a mezzo sistema informatico su rete TOR (internet anonimo)	massima	altissimo

2. Le opportunità

Al fine di ottemperare alla normativa cogente, Garda Uno ha già da tempo adottato una prima modalità di comunicazione a disposizione dei Segnalanti: attraverso uno specifico indirizzo email, un segnalante è messo in grado di inviare informazioni circostanziate afferenti un eventuale episodio ritenuto illecito secondo la normativa di riferimento.

Questa modalità di comunicazione non permette, come visto nelle premesse, di consentire la massima protezione possibile a chi, esponendosi in prima persona, potrebbe far emergere un episodio di illegalità che riveste la Società o uno o più Dipendenti/Amministratori della stessa. La conseguenza è la sostanziale non utilità (e conseguente non utilizzo) della modalità.

Al fine di poter superare questa criticità, sono state valutate le altre possibili opzioni che si sono ridotte, sostanzialmente, ad una sola possibilità: la messa a disposizione di un sistema informatico su rete TOR (internet anonimo).

3. Lo strumento: Globaleaks

Da anni l'Associazione italiana Hermes (https://www.hermescenter.org/home/about-mission/about-us/ Centro per la Trasparenza e i Diritti Umani) sta lavorando attivamente su scala mondiale su un progetto denominato "Globaleaks". Nel corso del 2016 è iniziata una stretta collaborazione con l'Autorità Anticorruzione italiana (ANAC) con l'obiettivo di mettere a disposizione degli Enti Pubblici e Privati uno strumento informatico in grado di poter ricevere segnalazioni di illegalità, poterle gestire nel rispetto della normativa e contemporaneamente garantire la riservatezza dei dati del Segnalante (una forma di Anonimato protetto). Il software Globaleaks è reso disponibile a tutta la comunità mondiale sotto forma di "sorgenti open-source" con lo scopo di coinvolgere tutti gli interessati (siano essi professionisti informatici, pubbliche amministrazioni, privati cittadini interessati) nel continuo sviluppo "a sorgenti

aperti" delle funzionalità e della sicurezza del software. Il fine è rendere disponibile per l'intera collettività mondiale (non solo italiana) una piattaforma uniforme, performante, sicura, funzionale e flessibile.
Lo sviluppo e il mantenimento di questo software da parte di Hermes è continuo e si avvale di numerosi esperti e sistemisti che hanno a cuore l'aspetto della difesa dei diritti umani nella Società Civile.
Questo software, infatti, viene utilizzato non solo ai fini delle segnalazioni di cui al tema di questo documento, ma anche per le segnalazioni di violazione dei diritti civili verso istituzioni mondiali (Amnesty International, giusto per citarne una) in numerosi paesi del mondo (da molti paesi africani alla Cina, al Sud America).
In Italia, questo sistema è utilizzato, per esempio e citando i "grandi" utilizzatori, da: ANAC, Agenza delle Entrate, Il Sole 24 Ore, Cameo, Fiorentina Calcio, Angelini, Comune di Milano oltre che una grande numerosità di altri Enti Locali, ASL, ecc.
Nel mondo è utilizzato anche e soprattutto per le segnalazioni a Amnesty International, Transparency International, molti siti di Giornalismo Investigativo, Autorità statali, Università pubbliche.
Questo viene citato soprattutto per sostenere la sicurezza dello strumento informatico che si sta implementando in Garda Uno.
Per quanto riguarda ANAC, nel corso dello scorso anno si è staccata dal gruppo di lavoro che sta portando avanti lo sviluppo e il mantenimento del Software creando un c.d. "fork" ovvero una derivazione a suo uso e consumo. Va detto che dal punto di vista meramente funzionale, la "versione" che ANAC sta mantenendo ha le medesime funzionalità della versione sviluppata dalla Comunità mondiale: la vera differenza sta nel cuore del software ovvero in ciò che non si vede. Oggi la versione

della Comunità ha raggiunto un livello di sofisticazione tale da rendere il sistema “autocontenitivo”: ovvero l’interfaccia di gestione, il database e il sistema di comunicazione con la rete anonima TOR sono contenuti in un unico “contenitore” che permette di evitare comunicazioni (potenzialmente intercettabili) tra diversi server dedicati, l’utilizzo delle ultime tecnologie e linguaggi ad elevata sicurezza e la possibilità di testare la sicurezza dell’ambiente attraverso società indipendenti esterne che eseguono periodici audit di penetration-test. Tutto questo permette di poter isolare il sistema in un server dedicato con soli 2 core, 2 Gb di Ram e 20 Gb di spazio disco con l’utilizzo di un Sistema Operativo open-source scalabile e sicuro in ambiente Unix-like.

Il 15 gennaio, ANAC ha deliberato la messa a disposizione con la modalità del c.d. “riuso” del software a tutte le realtà che ritengono di implementarlo. Purtroppo le specifiche tecniche ne rendono estremamente difficile l’implementazione; non ha infatti, purtoppo, i requisiti di leggerezza, sicurezza e scalabilità necessari ad una (relativamente) semplice implementazione: dalle specifiche tecniche pubblicate sarebbero necessari 3 diversi server con un totale di 24 core, 72 Gb di Ram e almeno 600 Gb di spazio disco oltre che notevoli richieste in termini di Sistema Operativo sempre unix-like ma con necessità di costose licenze di utilizzo.

4. La scelta: implementare con semplicità

Si è pertanto optato per la soluzione totalmente open-source: di relativa semplice implementazione, leggerezza nelle specifiche tecniche, elevatissima sicurezza intrinseca del sistema, scalabilità e, non ultimo, messa a disposizione dei segnalanti delle ultime tecnologie informatiche a difesa della riservatezza delle informazioni che questo vorrà fornire agli organi societari deputati a riceverle.

Si è acquisita la disponibilità di un piccolo server fisico presso una Server-Farm di un nostro Fornitore di Servizi Internet. Tale Server è sotto la nostra totale disponibilità e l'accesso è esclusivamente riservato all'Amministratore di Sistema (è stata identificata una specifica figura per questo specifico servizio) di Garda Uno. Il server è dedicato esclusivamente alle funzioni relative alla raccolta e alla gestione delle segnalazioni di condotta illecita; non sono stati installati ulteriori sottosistemi di comunicazione web o di rete come neppure logger di tracciamento delle connessioni. Il sistema è stato sottoposto ad un incremento del livello di sicurezza attraverso tutte le operazioni c.d. di "hardening" al fine di limitare al minimo possibile i rischi di intrusione. Il sistema operativo è configurato per autoaggiornarsi giornalmente ed è sottoposto ad un periodico monitoraggio da remoto da parte dell'Amministratore di Sistema.

Su questo sistema operativo è stato installato il Software Globaleaks e adeguatamente configurato. Le caratteristiche di sicurezza dello specifico software sono comprovate, come detto, dalle Società indipendenti incaricate di eseguire e rendicontare i "penetration-test" periodici.

Anche il software viene costantemente aggiornato al fine di mantenerne da un lato la piena disponibilità e fruibilità, dall'altro la sicurezza e l'evoluzione con nuove funzionalità.

5. Come funziona

Il funzionamento del software (che da ora chiameremo "piattaforma") prevede la presenza di 4 figure che hanno diverse funzioni e capacità di agire sulla piattaforma stessa.

Amministratore della Piattaforma:	ha il potere di configurare la piattaforma e monitorarne il corretto funzionamento; configura gli accessi per le due tipologie di ruolo che potranno avere accesso al sistema; non ha accesso ad alcuna informazione afferente le segnalazioni eventualmente inviate attraverso la piattaforma come neppure alle identità dei segnalanti

Riceventi:	sono le due entità interne alla Società che sono investite del potere di ricevere le segnalazioni: l'Organismo di Vigilanza e il Responsabile per la Prevenzione della Corruzione e la Trasparenza. Hanno accesso al contenuto delle segnalazioni; possono richiedere ulteriori informazioni al segnalante e "colloquiare" con esso per il tramite della piattaforma; non possono accedere direttamente alle informazioni riguardanti l'identità del segnalante che rimane non rivelato sino ad autorizzazione, se richiesta, del Custode delle Identità.
Custode delle Identità:	è l'entità (di solito) esterna alla Società che ha il potere di custodire e, se ritenuto, autorizzare la visibilità ai Riceventi dell'identità del segnalante a seguito di richiesta motivata per il tramite della piattaforma; non ha accesso ai contenuti della segnalazione e neppure all'identità del segnalante; il suo compito è valutare la motivazione dei Riceventi per concedere o meno la visibilità dell'identità (pertanto la motivazione deve essere articolata, particolareggiata)

Utente della piattaforma:	è il segnalante al quale, per il tramite della piattaforma, viene somministrato un questionario che permette da un lato di circostanziare correttamente l'evento oggetto di segnalazione e dall'altro scoraggiare (impedirlo è oggettivamente impossibile) l'uso improprio dello strumento.

Le comunicazioni tra la piattaforma e i Riceventi e il Custode delle Identità avviene con email crittografate per il tramite di una coppia di chiavi pubbliche/private personale.
Le comunicazioni tra la piattaforma (e comunque i Riceventi/Custode) e il segnalante riguardanti una specifica segnalazione avviene esclusivamente attraverso un codice di riferimento della segnalazione stessa assegnata dalla piattaforma che il Segnalante può utilizzare per accedere alla segnalazione e seguirne l'evoluzione nel tempo (ivi incluse le eventuali ulteriori richieste che i Riceventi possono inoltrare per approfondire l'istruttoria e la verifica della pratica).

I riceventi, nell'ambito delle loro prerogative, sulla base delle informazioni assunte per il tramite del segnalante col questionario, potranno svolgere tutte quelle indagini preliminari interne che potranno portare, se del caso, a valutare l'opportunità/dovere di investire del caso la Magistratura Penale e/o Contabile al fine di proseguire nelle indagini nelle forme previste dalla legge.

6. Potenziali sviluppi

Nell'ambito della collaborazione con i Comuni Soci di Garda Uno e con le Società Partecipate, può essere utilmente valutata la possibilità di fornire un supporto specifico in qualità di Servizio "tecnologico" di implementazione e mantenimento per gli Enti che ritengono di implementare per loro stessi il sistema predisposto per Garda Uno.

Attraverso l'acquisizione di un nuovo specifico server, è possibile sviluppare una specifica istanza separata per ogni Comune / Società richiedente in considerazione che il Software ha da poco integrato la possibilità di attivare separate istanze in modalità "multi-tenant".

Si ritiene che possa essere un Servizio interessante da proporre a fronte di un dispendio economico per l'Ente limitato.