**IL RUOLO DEL WHISTLEBLOWING NELLA CYBER SECURITY**

**di Alessandro Rodolfi - Università degli Studi di Milano**

Il termine anglossassone whistleblowing identifica l’istituto giuridico e le attività di regolamentazione volte a disciplinare **le procedure che incentivano e proteggono le persone che segnalano illeciti** oppure irregolarità.[[1]](#footnote-1) Caratteristiche chiave comuni al whistleblowing comprendono: la scoperta di illeciti legati al posto di lavoro, l’interesse pubblico, la segnalazione degli illeciti attraverso canali e/o persone designate, la buona fede e l’ esistenza di motivi ragionevoli. Si differenzia dal ***leaking****,* il quale è piuttosto caratterizzato da una «*falla in un sistema di comunicazione che fa fuoriuscire informazioni riservate che non dovrebbero circolare*»[[2]](#footnote-2) che da un processo strutturato di qualificazione delle segnalazioni e protezione delle fonti.

Il fattore cardine che ha dato impulso al whistleblowing in ambito cyber è rappresentato sicuramente dal fenomeno **WikiLeaks**: l’organizzazione capeggiata da Julian Assange ha avuto il merito indiscusso di stimolare l’attivismo utilizzando la rete e contribuendo alla nascita di tantissimi movimenti che hanno creato, più o meno efficacemente, piattaforme tecnologiche *web based* per promuovere la trasparenza democratica e segnalare abusi, illeciti, reati ed episodi di corruzione.

L’importanza del whistleblowing nella cyber security rileva principalmente sotto tre aspetti:

1. il primo è intrinseco allo strumento stesso e concerne la **privacy e la sicurezza informatica** che devono essere garantite dalla piattaforma tecnologica utilizzata per ricevere e gestire le segnalazioni;
2. il secondo è legato a una componente trasversale del processo di **cyber security risk management** con particolare riferimento alla comunicazione/consultazione e al monitoraggio/revisione;
3. Il terzo, allo stato attuale probabilmente più marginale, riguarda le **segnalazioni verticali** in tema di reati informatici, mancata compliance ICT e falle di sicurezza tecnologiche.

Sotto il primo aspetto è estremamente importante che la piattaforma tecnologica di whistleblowing risponda a **stringenti standard di ICT security** al fine primario di tutelare l’identità dei soggetti segnalanti e garantire la riservatezza delle informazioni contenute nella segnalazione. Non si deve mai dimenticare che a volte il whistleblower mette a rischio la propria stessa vita. Risultano dunque fondamentali architetture informatiche progettate fin dall’inizio per sfruttare tecniche di protezione dei dati basate su **crittografia** **allo stato dell’arte** e **tecnologie di anonimato nelle comunicazioni** dirette alla salvaguardia dell’origine informatica della segnalazione. Il rispetto di misure di sicurezza applicative, l’uso di componenti tecnologiche assoggettate a molteplici **test di sicurezza**, la **revisione del codice** e le attività di **peer review** rappresentano best practices oggi irrinunciabili. Altrettanto importanti sono la messa in atto di molteplici misure di prevenzione di attacchi di negazione e saturazione dei servizi (DDOS) che possano garantire la disponibilità del sistema.

La ricezione e l’analisi delle segnalazioni dovrebbe poi essere consentita solo ad un ristretto nucleo di persone per diminuire i rischi derivanti dall’accesso a una banca dati sicuramente critica. La gestione del controllo degli accessi, dell’autenticazione informatica e della profilazione degli utenti dovrebbe seguire criteri particolarmente rigidi tali da non permettere l’accesso ai dati in chiaro ai soggetti non autorizzati, agli amministratori di sistema, ai soggetti che possano accedere alla base dati del sistema.

Interessanti considerazioni in merito si trovano all’interno di un recente documento dell’OCSE “***Digital Security Risk Management for Economic and Social Prosperity***”[[3]](#footnote-3). Il paper, oltre che richiamare l’approccio basato sui rischi degli ISO standard 31000 e 27001 (argomento che verrà approfondito successivamente), fornisce spunti in merito all’applicazione delle **misure di sicurezza digitali riguardo alla tutela dei diritti umani e dei valori fondamentali delle persone** «*Depending on how they are used, security measures adopted to manage digital security risk can positively affect or undermine human rights and fundamental values. They can affect freedom of expression, the free flow of information, the confidentiality of information and communications, the protection of privacy and personal data, openness and fair process. For example,* ***security measures can enhance privacy protection, or provide anonymity to whistle-blowers and human rights activists****. They can also enable the illegitimate monitoring of citizens, or prevent access to activists’ content. They can affect other rights and values not listed in the Principle. Therefore, a responsible approach requires that decisions to manage digital security risk be made in light of their consequences on these rights and values».*

Il secondo tema parte dalla riflessione che la gestione del rischio cyber non può più essere considerata disgiunta dal generale contesto di rischio aziendale e soprattutto non deve restare confinata nell’area di Information Technology**. La cyber security deve essere vista come un fattore strategico per la *governance* aziendale**: sono sotto gli occhi di tutti gli enormi danni causati da attacchi informatici sempre più sofisticati che comportano la sottrazione di proprietà intellettuale, rilevanti problematiche reputazionali, cause legali derivanti da contenziosi o pesanti oneri sanzionatori. In alcuni settori, per esempio quello finanziario, il legislatore ha già previsto che l’organo con funzione di supervisione strategica (*il board*) sia responsabile dell’indirizzo e del controllo dell’ analisi del rischio informatico dovendone approvare per esempio la metodologia e verificare la propensione agli eventi avversi.[[4]](#footnote-4)

Il processo di gestione del rischio che l’*International Organization for Standardization* (ISO) ha imposto a tutti i sistemi di gestione (primo fra i quali quello relativo alla sicurezza delle informazioni **ISO 27001** a partire dal 2013) è rappresentato nello standard internazionale **ISO 31000**: definizione del contesto, valutazione del rischio (che comprende le fasi di identificazione, analisi e ponderazione) e trattamento del rischio; i sistemi di whistleblowing entrano in gioco in maniera trasversale per poter interagire efficacemente con ogni singola fase del processo di gestione del rischio. Nel dettaglio:

1. **comunicazione e consultazione** (punto 5.2): in riferimento allo sviluppo e al mantenimento di appropriati meccanismi di reporting con stakeholder interni ed esterni;
2. **monitoraggio e riesame** (punto 5.6): per rilevare cambiamenti nel contesto esterno ed interno, evidenziare modifiche ai criteri di rischio e al rischio stesso, identificare nuovi rischi emergenti, analizzare ed apprendere dalle segnalazioni pervenute, fornire e alimentare gli indicatori chiave di prestazione.[[5]](#footnote-5)

La funzione dei sistemi di whistleblowing a supporto di una corretto processo di gestione del rischio di cyber security risulta dunque fondamentale poiché da un lato stimola i rapporti con tutti i portatori di interesse, rappresentati da vari soggetti molto attivi nello scenario del ciberspazio, per la costruzione iniziale di una “robusta” piattaforma di whistleblowing e dall’altro consente il costante monitoraggio dell’applicazione delle security policy, delle misure di sicurezza da parte delle organizzazioni, della compliance ICT security in generale. Attualmente la legislazione italiana in ambito pubblico prevede che una misura di contrasto alla corruzione sia rappresentata dalla stesura del “**Piano Nazionale Anticorruzione**” il quale deve contenere alcune indicazioni in merito alle procedure di whistleblowing[[6]](#footnote-6): anche se probabilmente residuale al contesto di cyber security, non è da escludersi che possano pervenire attraverso questi canali, illeciti che riguardano la materia oggetto di trattazione in questo articolo.

Dal terzo punto di vista l’applicazione del whistleblowing nel cyber security risk management rileva attualmente soprattutto in ambiti di **business regolamentati con una forte focalizzazione nel mondo ICT e nella gestione di informazioni digitali classificate**: si potrebbe trattare di organizzazioni quotate in borsa[[7]](#footnote-7), appartenenti al settore finanziario[[8]](#footnote-8), sottoposte alla compliance di cui al **D. Lgs. n. 231/2001** sulla responsabilità penale degli enti oppure aziende certificate ISO 27001. Un esempio potrebbe essere rappresentato da una segnalazione riguardante uno dei reati informatici previsti dalla 231 indirizzata all’Organismo di Vigilanza.[[9]](#footnote-9)

Scenari futuri sono applicabile anche al settore ***automotive*** come recentemente segnalato da Mary Barra, Amministratore Delegato di General Motors[[10]](#footnote-10), secondo la quale è necessaria una vera e propria coalizione tra le case automobilistiche e i legislatori per contrastare il rischio cyber crime: gli attacchi diretti verso le auto, sempre più connesse alla rete e con tecnologie di guida assistita «diventerà un problema di sicurezza pubblica». Non a caso la nuova *release* di un altro standard internazionale di settore l’**ISO/TS 16949** prevederà espressamente l’istituzione di canali di whistleblowing.

Infine è del tutto probabile che nascano **iniziative specifiche** di whistleblowing fortemente focalizzate alla raccolta di segnalazioni attinenti alle tematiche del cyber crime.

1. Una definizione più dettagliata proviene dall’autorevole ente di normazione inglese British Standards Institute fornisce nel documento “PAS 1998:2008 Whistleblowing Arrangements Code of pratice” è la seguente: «Whistleblowing is the popular term used when someone who works in or for an organization raises a concern about a possible fraud, crime, danger or other serious risk that could threaten customers, colleagues, shareholders, the public or the organization’s own reputation». [↑](#footnote-ref-1)
2. Per un approfondimento in merito si veda, G. Ziccardi, INTERNET, CONTROLLO E LIBERTA’ - Trasparenza, sorveglianza e segreto nell'era tecnologica, Milano, Raffaello Cortina Editore, 2015. [↑](#footnote-ref-2)
3. Per un approfondimento https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm (sito web consultato, e documento disponibile online, il 27 luglio 2016). [↑](#footnote-ref-3)
4. Circolare 263 15° aggiornamento della Banca d’Italia. [↑](#footnote-ref-4)
5. Rif. ISO 31004 “*Risk management - Guidance for the implementation of ISO 31000*”. [↑](#footnote-ref-5)
6. Da notare che tra gli allegati che sono stati stilati con l’intendo di fornire alle P.A. «approfondimenti

   di carattere interpretativo, procedurale e metodologico» si possono evincere diversi spunti per coadiuvare le amministrazioni nella gestione del rischio: l’all. n. 6, in particolare, fa esplicito riferimento allo standard ISO 31000. Per un approfondimento http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/Anticorruzione (sito web consultato, e documento disponibile online, il 27 luglio 2016). [↑](#footnote-ref-6)
7. Il Codice di Autodisciplina della Borsa Italiana prevede che «un adeguato sistema di controllo interno e di gestione dei rischi debba essere dotato di un sistema interno di segnalazione da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistemi di whistleblowing) in linea con le best practices esistenti in ambito nazionale e internazionale, che garantiscano un canale informativo specifico e riservato nonché l’anonimato del segnalante». [↑](#footnote-ref-7)
8. Nel luglio 2015 l’11° aggiornamento della Circolare n. 285 da parte della Banca d’Italia integra nel sistema dei controlli interni «i sistemi interni di segnalazione delle violazioni (c.d. whistleblowing)». [↑](#footnote-ref-8)
9. DDL C. 3365-A approvato alla Camera il 21/01/2016 prevede l’inserimento della disciplina in ambito privato all’interno del D. Lgs. n. 231/2001. [↑](#footnote-ref-9)
10. Rif. http://www.ansa.it/canale\_motori/notizie/attualita/2016/07/25/ad-general-motors-cyberattacchi-ad-auto-minaccia-crescente\_5c7e16c4-64b5-4118-b754-251e2ed94ba8.html. [↑](#footnote-ref-10)