

Il DENARO.it

Soldi & Imprese

8-07-2006

l'impresa nell'era dell'informazione

Privacy e crimini d'impresa

Riccardo e Rosario Imperiali

Esiste una nuova frontiera di controllo aziendale sull'attività dei dipendenti che non rientra nella sfera di discrezionalità imprenditoriale: si tratta di ispezioni e verifiche "obbligate" da esigenze di conformità a normative nazionali e internazionali.

Una di queste riguarda la procedura di segnalazione di fatti/comportamenti aziendali ritenuti moralmente censurabili rispetto agli obblighi di trasparenza finanziaria imposti, ormai, a livello globale.

Decreto 231

In Italia, il decreto legislativo 231/2001 prevede, tra gli adempimenti legati al modello organizzativo di gestione del rischio penale d'impresa, obblighi di informazione - delle varie funzioni aziendali - verso l'organismo interno preposto a vigilare sull'effettività ed efficacia del modello.

Il decreto nulla dice, tuttavia, in ordine alla tipologia di informazioni rilevanti che possono spaziare da semplici anomalie di alcuni dati economici (ad esempio, l'incremento del budget destinato all'omaggistica) a vere e proprie ipotesi di reato imputabili a persone determinate (procedimenti penali avviati dall'autorità giudiziaria a carico di dirigenti o dipendenti).

Informazioni di questo tipo, in particolare, richiedono gli adempimenti e le garanzie previste dal codice privacy, a tutela dei dati personali.

Sarbanes Oxley Act

Negli Usa, il Sarbanes Oxley Act (Sox) prevede, da un lato, obblighi di report più circoscritti — legati all'area di gestione della contabilità e dei bilanci — dall'altro individua modalità di segnalazione più incisive e penetranti: tutte le aziende quotate sui mercati americani — e, quindi, anche le aziende europee e italiane - devono dotarsi di un'apposita funzione di controllo interno (Audit Committee) abilitata a ricevere segnalazioni di condotte moralmente sospette e potenzialmente rivelatrici di illeciti in materia di gestione contabile, revisione e controlli contabili interni.

Si tratta di veri e propri sistemi di delazione - non a caso indicati, dalle norme Usa, come "whistleblowing schemes" (procedure di "soffiata") — nei quali la tutela del delatore contro possibili forme di ritorsione prevale — anzi prevarica - sulla protezione della persona oggetto della segnalazione.

Privacy

Questo sbilanciamento della legge americana — dovuto al timore di scongiurare in ogni modo crack finanziari di vasta portata — pone seri problemi di compatibilità con le norme europee sul data protection basate sul principio fondamentale di non discriminazione: chiunque, anche se oggetto di whistleblowing, ha diritto alla protezione dei dati personali che lo riguardano. Il che impone alle aziende italiane quotate oltre oceano, così come alle filiali italiane di holding americane, di conciliare la conformità alla "legge Sox" con le norme del codice privacy, vincolanti per tutte le imprese stabilite in Italia.

Codice

Il codice privacy esonera aziende ed enti dall'obbligo di acquisire il consenso degli interessati quando l'uso dei dati personali si renda necessario per soddisfare obblighi posti da norme di legge o regolamento, compresa la normativa comunitaria. Questa esimente non consente, tuttavia, di legittimare tout court le procedure di segnalazione di illeciti del "tipo Sox", ove non siano recepite da norme comunitarie o nazionali. In caso contrario, qualunque norma extra-Ue potrebbe eludere facilmente il sistema comunitario per la tutela dei dati personali.

La distonia tra norme americane e norme europee richiede un preventivo bilanciamento di interessi rimesso alle Autorità nazionali di protezione dei dati personali (in Italia, il Garante privacy): le policy aziendali di conformità al SOX — con i relativi meccanismi di segnalazione e reporting all'organismo di vigilanza — comportano un livello esponenziale di rischio per la dignità delle persone oggetto della segnalazione. Si impone, perciò, una verifica preliminare (c.d. prior checking) del Garante, volta a configurare la cornice di legittimità data protection su cui l'azienda può innestare le procedure di segnalazione delle irregolarità contabili prescritte dalla legge americana.

Interesse

Una volta definita, col supporto del Garante, la cornice di legittimità del whistleblowing, l'azienda può acquisire da terzi "segnalatori" — che spesso restano anonimi — informazioni delicate sul conto di amministratori, manager, funzionari e dipendenti nei confronti dei quali viene avviata, il più delle volte, un'indagine interna riservata. In questa fase, l'interesse aziendale per una verifica "a fari spenti" prevale sul diritto della persona "segnalata" alla trasparenza informativa e, di conseguenza, sulla necessità di acquisirne preventivamente il consenso al trattamento dei propri dati personali.

Non a caso, lo stesso codice privacy — così rigoroso nel prescrivere obblighi e garanzie a tutela delle persone dei cui dati si tratta — ammette la possibilità di prescindere non solo dall'informativa ma anche dal consenso dell'interessato, quando i dati sono trattati in vista di una finalità di difesa in giudizio che — nei casi previsti dal decreto 231 e dalla legge SOX — coinvolge l'azienda anche sul piano della responsabilità penale/amministrativa, per fatti commessi dal management nell'interesse o a vantaggio dell'ente.

Diritti individuali

La tutela dei diritti delle persone coinvolte rientra in una logica di bilanciamento "a doppio binario": da un lato, tale tutela si comprime inevitabilmente nella fase di verifica interna e dell'eventuale necessità aziendale di azione o difesa in giudizio, per riespandersi, una volta cessata l'emergenza istruttoria.

Qualora sia esaurita l'esigenza di tutelare i propri diritti difensivi, elemento che congela provvisoriamente talune tutele "privacy", l'interessato recupera la pienezza dei propri diritti: potrà accedere ai dati oggetto della segnalazione — escluso il nominativo del delatore — chiedere la rettifica dei dati inesatti, incompleti o non aggiornati e, soprattutto, la cancellazione di quei dati per i quali è cessato lo scopo di conservazione.

Per altro verso, l'azienda è tenuta a gestire la procedura di segnalazione secondo la consueta metodologia data protection: l'adozione di ruoli privacy nell'ambito del trattamento "whistleblowing" e la predisposizione di rigorose misure di sicurezza sono adempimenti preordinati ad un principio di civiltà: che il fatto, puro e semplice, della segnalazione non arrechi alcun pregiudizio al "segnalato" e al "segnalante", in termini di esposizione alla "gogna" del gossip aziendale.

