



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Segnalazione al Parlamento e al Governo [art. 154, 1 f) del Codice] - 10 dicembre 2009

Bollettino del n. 111/dicembre 2009, pag. 0

[doc. web n. 1693019]

Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale - 10 dicembre 2009
(art. 154, comma 1, lett. f), d.lg. 30 giugno 2003, n. 196)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1. Recenti scandali economico-finanziari che hanno coinvolto società di capitali ammesse alle negoziazioni in mercati regolamentati (si pensi, tra gli altri, ai casi "Enron", "Parmalat", "Tyco" e "Worldcom") hanno richiamato l'attenzione, soprattutto sul piano sovranazionale, sulla necessità del miglioramento delle pratiche di "corporate governance", nel quadro di una più ampia strategia di gestione e minimizzazione del rischio da parte degli operatori economici, oltre che di salvaguardia della stessa stabilità dei mercati finanziari.

Anche al fine di prevenire il ripetersi di scandali di portata internazionale, in alcuni ordinamenti sono state introdotte normative (ad esempio, il *Sarbanes-Oxley Corporate Reform Act* adottato negli Stati Uniti, ovvero il *Public Interest Disclosure Act* presente in Gran Bretagna) che prevedono, tra l'altro, l'adozione di sistemi e procedure di segnalazione (c.d. *whistleblowing*) di presunti illeciti –riconducibili in particolare, a fenomeni di corruzione o frode– ascrivibili a soggetti operanti a vario titolo all'interno di aziende operanti sul mercato, con il contestuale inserimento di misure a protezione degli autori (in buona fede) della segnalazione.

Tali procedure (e i successivi approfondimenti conoscitivi effettuati mediante attività di verifica e indagine a cura di linee organizzative a ciò appositamente dedicate) riguardano generalmente ambiti particolarmente delicati all'interno delle menzionate aziende e rientrano tra le misure organizzative approntate per contrastare fenomeni gravi quali la corruzione e altre forme di lotta alla criminalità bancaria e finanziaria, anche attraverso la vigilanza sulla regolare tenuta della contabilità.

L'adozione di siffatti sistemi di segnalazione è stata accompagnata dalla contestuale previsione di misure poste a presidio degli autori delle segnalazioni effettuate "in buona fede" (*in good faith*), volte a scongiurare in capo agli stessi il rischio di licenziamento o il verificarsi di altre conseguenze pregiudizievoli in relazione al rapporto di lavoro; ciò, anche in considerazione della particolare delicatezza delle informazioni trattate, che recano con sé un elevato rischio di stigmatizzazione e vittimizzazione del soggetto "segnalato e, in ipotesi, anche del "segnalante".

Considerata la progressiva diffusione di tali sistemi anche presso società italiane –sovente veicolata dall'introduzione di analoghi modelli organizzativi all'interno di società per lo più operanti a livello di multinazionali– vengono di seguito indicate le ragioni per le quali al Garante sembrerebbe opportuno un intervento normativo volto a fornire un'idonea e sistematica base normativa nonché a disciplinare i profili di interferenza di tale fenomeno con la disciplina di protezione dei dati personali contenuta nel decreto legislativo 30 giugno 2003, n. 196.

2. La tematica in esame è stata recentemente oggetto di numerose istanze (quesiti, pareri, verifiche preliminari) indirizzate all'Autorità al fine di ottenere una valutazione in ordine alla liceità e alle modalità di effettuazione dei trattamenti svolti nell'ambito delle menzionate procedure di segnalazione.

Con espresso riferimento alla disciplina di protezione dei dati personali, tale tematica è stata affrontata dal Gruppo dei Garanti europei costituito ai sensi dell'art. 29 della direttiva 95/46/Ce, che, con proprio parere reso il 1° febbraio 2006, ha fornito preliminari indicazioni per rendere i trattamenti di dati personali effettuati per il tramite dei menzionati sistemi di segnalazione conformi ai principi contenuti nella citata direttiva.

Per quanto qui d'interesse, si rappresentano di seguito, in via del tutto schematica, i profili di particolare rilevanza evidenziati dal Gruppo ex art. 29:

- *ambito di applicazione*: l'ambito di applicazione dei sistemi di segnalazione è stato circoscritto (in attesa di successivi approfondimenti da parte dello stesso Gruppo e coerentemente con le finalità perseguite dalla citata *Sarbanes-Oxley Corporate Reform Act*) ai soli illeciti riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria;
- *presupposti di liceità del trattamento*: il trattamento può considerarsi lecito ove ricorrano alcuni specifici presupposti individuati dall'art. 7 della direttiva (segnatamente riconducibili alla necessità di dare adempimento a un obbligo legale, ovvero di perseguire un legittimo interesse del responsabile –*id est*: del titolare– del trattamento o di terzi);

- *esercizio del diritto di accesso da parte dell'interessato*: tale diritto può essere limitato per garantire la tutela dei diritti e delle libertà altrui, con la precisazione che *"in nessuna circostanza può essere permesso al denunciato di avvalersi del suo diritto di accesso per ottenere informazioni sull'identità del denunciante"* (salvo la malafede di quest'ultimo);
- *denunce anonime*: pur privilegiandosi la strada delle denunce nominative, risultano ammissibili anche le denunce anonime, purché ricorrano alcune condizioni espressamente indicate e vengano adottate opportune precauzioni (vaglio preventivo di ammissibilità; eventuale trattazione più rapida; ecc.).

3. Con riferimento all'ordinamento italiano, pur in assenza di una disciplina legislativa appositamente dedicata alla materia, è possibile ritrovare nel sistema una serie di riferimenti normativi che possono contribuire a consentire (e in qualche misura a giustificare) l'eventuale adozione di meccanismi di segnalazione riconducibili al fenomeno del *whistleblowing*.

Deve, al riguardo, considerarsi che i sistemi di segnalazione possono servire a tutelare sia interessi "esterni" all'azienda, avere cioè finalità di tutela di ordine generale del sistema (per esempio, tutela della stabilità dei mercati finanziari, lotta alla corruzione, contrasto alla criminalità economica e finanziaria, tutela dei risparmiatori), sia interessi "interni" all'azienda (in relazione all'obbligo di correttezza e fedeltà di tutti coloro che collaborino a vario titolo all'attività aziendale, con particolare riguardo alla tutela del segreto industriale e aziendale).

Quanto alle finalità di tutela di ordine generale, può farsi riferimento alla disciplina contenuta nel d.lg. 8 giugno 2001, n. 231 in materia di responsabilità amministrativa (susceptibile di insorgere in capo alle società e ad altri soggetti privi di personalità giuridica per talune fattispecie di reato commesse nell'interesse o a vantaggio dell'ente da persone operanti in posizione apicale nell'impresa o da persone sottoposte alla loro direzione o vigilanza).

Per quanto concerne le menzionate finalità "interne" all'azienda, invece, si può fare riferimento ad alcune disposizioni del codice civile che solo indirettamente (e per profili parziali e circoscritti) possono prestarsi a disciplinare alcuni aspetti del fenomeno in questione. Il richiamo, in particolare, è all'art. 2105 cod. civ., che, pur disciplinando l'obbligo di fedeltà del prestatore di lavoro –concretizzando in modo puntuale la clausola generale di correttezza di cui agli artt. 1175 e 1375 del codice medesimo, come evidenziato anche dalla Corte di Cassazione (ad esempio nella sentenza n. 7819 del 2001)– costituisce invero espressione di un più generale dovere di lealtà riferibile a tutti coloro che operano a vario titolo nell'organizzazione aziendale.

Merita infine rilevare, per quanto concerne in particolare il segnalante, che i presupposti atti a giustificare un possibile intervento possono essere genericamente rinvenuti, anche secondo quanto recentemente statuito dalla Corte europea dei diritti dell'uomo, nell'ambito del diritto alla libera manifestazione del pensiero (art. 21 della Costituzione; in termini similari, la sentenza della CEDU del 12 febbraio 2008, *Guja v. Moldova*).

3.1. L'eterogeneità dei riferimenti sopra richiamati attesta che non è possibile rinvenire fondamenti normativi sistematici atti a regolare il fenomeno. In questo contesto un eventuale intervento del Garante avrebbe un carattere necessariamente parziale e limitato e comporterebbe inevitabilmente l'adozione di scelte, relative in particolare agli ambiti di applicazione, che appare più opportuno rimettere al Parlamento, come si chiarirà meglio al paragrafo che segue. Inoltre, un'espressa disciplina normativa offrirebbe una positiva soluzione alle criticità che il fenomeno in questione comporta in rapporto alla vigente normativa sulla protezione dei dati personali.

4. Alla luce dell'incerto quadro normativo sopra delineato, il primo profilo problematico, con particolare riferimento alla disciplina di protezione dei dati personali, attiene ai presupposti di liceità del trattamento che verrebbe posto in essere mediante l'adozione dei predetti sistemi di segnalazione. Non potendo sostenersi che la segnalazione avverrebbe per la necessità di adempiere ad un obbligo legale (di cui, come detto, non vi è chiara enunciazione nell'ordinamento), un trattamento di dati personali di questo tipo, da attuare evidentemente in assenza del consenso degli interessati, potrebbe in astratto essere lecito sulla base di un provvedimento di *"bilanciamento di interessi"* da parte di questa Autorità (ai sensi dell'art. 24, comma 1 lett. g), del Codice in materia di protezione dei dati personali). Bilanciamento che potrebbe basarsi unicamente sulla finalità di *"perseguire un legittimo interesse del titolare del trattamento o di un terzo"* (quale potrebbe essere, nel caso di specie, la garanzia della stabilità dei mercati finanziari, il contrasto a fenomeni di corruzione ecc.).

E' evidente che in questo caso l'intervento del Garante avverrebbe comunque in un quadro di riferimento incerto e generico e comporterebbe delicate scelte volte a "perimetrare" l'ambito di applicazione della nuova disciplina. Scelte che, peraltro, sarebbero comunque condizionate dallo stesso Codice, dal momento che la citata norma di riferimento (art. 24) non consente di ricomprendere, nell'ambito di un eventuale provvedimento di bilanciamento di interessi, talune specifiche tipologie di trattamento.

Ulteriori criticità sono poi ravvisabili in relazione all'estensione del diritto di accesso da parte del soggetto "segnalato" (con particolare riferimento al diritto di conoscere l'origine dei dati e, segnatamente, quelli identificativi dell'autore della segnalazione), nonché all'eventuale idoneità delle segnalazioni anonime ad attivare procedure interne di controllo.

In astratto, la vigente disciplina di protezione dei dati attribuisce all'interessato (in questo caso il soggetto a cui si riferisce la segnalazione) il "diritto" di conoscere l'origine dei dati (cfr. art. 7, comma 2, lett. a), del Codice, in attuazione dell'art. 12, par. 1, lett. a), 2° alinea, della direttiva 95/46/Ce che, al riguardo, attribuisce all'interessato il diritto di ottenere la comunicazione di *"tutte le informazioni disponibili sull'origine dei dati"*).

L'applicazione in concreto, nell'ambito qui considerato, di tale previsione rischierebbe di infirmare l'efficacia dei menzionati sistemi di segnalazione, potendo dissuadere i segnalanti dal mettere al corrente le linee organizzative preposte circa gli illeciti eventualmente posti in essere all'interno dell'organizzazione di appartenenza.

Problematica risulta altresì l'ammissibilità dei trattamenti derivanti da eventuali segnalazioni "anonime"; le stesse, come sottolineato anche dal Gruppo dei Garanti europei, potrebbero infatti prestarsi ad usi strumentali, con il rischio di alimentare all'interno dell'ambiente lavorativo una cultura della delazione. Si aggiunga, inoltre, che l'anonimato non consentirebbe al titolare del trattamento di raccogliere ulteriori e più precise indicazioni in relazione alle vicende segnalate, utili alle verifiche da effettuare.

5. In ragione dell'incertezza normativa che caratterizza la materia oggetto della presente segnalazione (e dei profili di criticità più strettamente riferiti alla vigente disciplina di protezione dei dati personali), il Garante auspica dunque che gli aspetti sopra individuati connessi all'impiego e al funzionamento dei citati sistemi di segnalazione possano trovare una puntuale regolamentazione con l'individuazione di una disciplina legislativa che assicuri un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di trasparenza e di tutela delle aziende presso le quali questi operano, anche per quanto concerne i possibili riflessi sui mercati di riferimento.

Possibilità, questa, peraltro conforme alla previsione di cui all'art. 5 della stessa direttiva 95/46/Ce, che rimette agli Stati membri la precisazione delle "condizioni alle quali i trattamenti di dati personali sono leciti".

PER QUESTE RAGIONI

il Garante segnala al Parlamento e al Governo l'opportunità che sia valutata, in relazione all'utilizzo di sistemi di segnalazione di presunti illeciti commessi da soggetti operanti a vario titolo nell'ambito di un'organizzazione aziendale, l'adozione di apposite disposizioni legislative volte a:

- individuare i presupposti di liceità del trattamento effettuato per il tramite dei citati sistemi di segnalazione, in particolare delineando una base normativa che definisca, innanzi tutto, l'ambito soggettivo di applicazione della disciplina e le finalità che si intendono perseguire;
- valutare in particolare, nel processo di perimetrazione sul piano soggettivo della disciplina, se estenderla a ogni tipo di organizzazione aziendale ovvero, per esempio, riferirla alle sole società ammesse alle negoziazioni su mercati regolamentati;
- individuare nell'ambito dei soggetti operanti a vario titolo all'interno delle società coloro che possono assumere la qualità di soggetti "segnalati";
- individuare in modo puntuale le finalità che si intendono perseguire e le fattispecie oggetto di possibile "denuncia" da parte dei segnalanti;
- definire la portata del diritto di accesso previsto dall'art. 7 del Codice da parte del soggetto al quale si riferisce la segnalazione (interessato), con riguardo ai dati identificativi dell'autore della segnalazione (denunciante);
- stabilire l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

Roma, 10 dicembre 2009

stampa

chiudi