



00195/06/IT

WP 117

Parere 1/2006 relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria

Adottato il 1° febbraio 2006

Il Gruppo è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente, che si occupa della protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE.

Il servizio di segretariato è fornito dalla Direzione C (Giustizia civile, diritti e cittadinanza) della Commissione europea, Direzione generale Giustizia, Libertà e Sicurezza, B-1049, Bruxelles, Belgio, Ufficio No LX46 1/143.

Sito web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

INDICE

I.	INTRODUZIONE	4
II.	GIUSTIFICAZIONE DELL'OGGETTO LIMITATO DEL PARERE	5
III.	ENFASI PARTICOLARE POSTA DALLA NORME SULLA PROTEZIONE DEI DATI SULLA PROTEZIONE DELLA PERSONA DENUNCIATA	6
IV.	COMPATIBILITÀ DELLE PROCEDURE DI DENUNCIA CON LE NORME SULLA PROTEZIONE DEI DATI.....	7
1.	<i>Legittimità dei sistemi di denuncia (articolo 7 della direttiva 95/46/CE)</i>	7
	i) Il sistema di denuncia è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento (articolo 7, lettera c)).....	7
	ii) Il sistema di denuncia è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento (articolo 7, lettera f))	8
2.	<i>Applicazione del principio relativo alla qualità dei dati e del principio di proporzionalità (articolo 6 della direttiva sulla protezione dei dati)</i>	9
	i) Possibile limitazione del numero di soggetti autorizzati a denunciare presunte irregolarità o violazioni dell'etica di comportamento.....	10
	ii) Possibile limitazione del numero di soggetti denunciabili	10
	iii) Promozione delle denunce nominative e riservate rispetto alle denunce anonime	10
	iv) Proporzionalità e esattezza dei dati rilevati e trattati	12
	v) Osservanza dei termini di conservazione dei dati.....	12
3.	<i>Informativa chiara e completa sulla procedura (articolo 10 della direttiva sulla protezione dei dati)</i>	13
4.	<i>Diritti del denunciato</i>	13
	i) Diritti di informazione.....	13
	ii) Diritto di accesso, di rettifica e di cancellazione.....	14
5.	<i>Sicurezza dei trattamenti (articolo 17 della direttiva 95/46/CE)</i>	14
	i) Misure di sicurezza pertinenti.....	14
	ii) Riservatezza delle segnalazioni effettuate attraverso procedure interne di denuncia	14
6.	<i>Gestione delle procedure di denuncia.....</i>	15
	i) Organizzazione specifica interna della gestione delle procedure di denuncia.....	15
	ii) Possibilità di ricorrere a fornitori esterni	16
	iii) Principio di verifica nell'UE per le imprese europee e eccezioni	16

7. <i>Trasferimenti verso paesi terzi</i>	17
8. <i>Adempimento degli obblighi di notificazione</i>	17
V – CONCLUSIONI	18

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,¹

visti gli articoli 29 e 30, paragrafi 1, lettera a), e 3 della richiamata direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

Il presente parere contiene indicazioni su come attuare le procedure interne di denuncia nel rispetto delle norme UE sulla protezione dei dati di cui alla direttiva 95/46/CE².

I vari problemi riscontrati nell'applicare tali procedure in Europa nel 2005, anche in relazione alla protezione dei dati, mostrano che lo sviluppo di questa pratica in tutti i paesi dell'UE può incontrare difficoltà sostanziali, dovute principalmente a diversità culturali dipendenti a loro volta da ragioni storiche e/o sociali che non possono essere misconosciute né ignorate.

Il Gruppo sa che queste difficoltà sono in parte legate all'ampia gamma di problemi che è possibile segnalare attraverso le procedure interne di denuncia, che tali procedure comportano in alcuni paesi dell'UE difficoltà specifiche inerenti a aspetti del diritto del lavoro e che sono in corso lavori in proposito, che bisognerà approfondire. Il Gruppo deve altresì tenere conto del fatto che in alcuni paesi dell'UE il funzionamento delle procedure di denuncia è regolamentato per legge, mentre in quasi tutti gli altri paesi non esistono norme o regolamenti specifici.

Di conseguenza, il Gruppo reputa prematuro, allo stadio attuale, adottare un parere definitivo sulla denuncia delle irregolarità in generale. Con il presente parere ha deciso di affrontare quegli aspetti per i quali è più urgente un orientamento a livello dell'UE. Considerato ciò e per le ragioni esposte nel documento, il presente parere si limita formalmente all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria.

¹ GUL 281 del 23.11.1995, pag. 31, disponibile al seguente indirizzo:
http://europa.eu.int/comm/internal_market/privacy/law_en.htm

² Nei limiti del mandato specifico del gruppo, il presente documento di lavoro non affronta altre difficoltà giuridiche poste dalle procedure di gestione delle denunce, specie in relazione al diritto del lavoro e al diritto penale.

Il Gruppo ha adottato il presente parere ben sapendo di dover esaminare più a fondo l'eventuale compatibilità delle norme UE sulla protezione dei dati con le procedure interne di denuncia in settori diversi da quelli appena citati, come le risorse umane, la salute e la sicurezza dei lavoratori, il danno e i rischi ambientali e la commissione di reati. Proseguirà perciò tale sua disamina nei prossimi mesi per stabilire se siano necessari orientamenti comunitari anche in quei settori, eventualmente integrando o adattando in un successivo documento i principi enucleati nel presente parere.

II. GIUSTIFICAZIONE DELL'OGGETTO LIMITATO DEL PARERE

Il Congresso degli Stati Uniti ha emanato nel 2002 la legge Sarbanes-Oxley (*Sarbanes-Oxley Act* o "SOX") a seguito di una serie di scandali finanziari che hanno coinvolto grandi imprese.

Tale legge fa obbligo alle imprese statunitensi ad azionariato diffuso, alle loro controllate con sede nell'UE e alle società straniere quotate in uno dei mercati finanziari degli USA di adottare nell'ambito del rispettivo comitato per la revisione dei conti "*procedure per la ricezione, l'archiviazione e il trattamento di denunce ricevute dalla Società e riguardanti la tenuta della contabilità, i controlli contabili interni e la revisione contabile, nonché per la presentazione in via confidenziale o anche anonima di lamentele da parte di dipendenti in merito a pratiche contabili o di revisione censurabili*"³. Inoltre, la sezione 806 SOX contiene disposizioni dirette a garantire che i dipendenti di società negoziate su mercati regolamentati che comprovino l'esistenza di frodi non siano soggetti ad alcuna forma di ritorsione per essersi avvalsi di tali sistemi di segnalazione⁴. L'applicazione di tale legge è soggetta al controllo della SEC (*Securities and Exchange Commission*).

Le norme del Nasdaq⁵ e del NYSE (*New York Stock Exchange*)⁶ contengono disposizioni analoghe. Le società che sono quotate al Nasdaq o al NYSE sono tenute a certificare ogni anno, su quei mercati, i propri bilanci. Tale processo di certificazione implica che le aziende sono nella posizione di affermare che ottemperano a una serie di norme, comprese quelle sulla denuncia delle irregolarità.

Il Nasdaq, il NYSE e la SEC impongono pesanti sanzioni e penalità alle società che non si conformano ai requisiti prescritti in materia di denuncia. Sussistendo motivi di incertezza quanto alla compatibilità delle procedure di denuncia con le norme dell'Unione sulla protezione dei dati, le aziende interessate corrono il duplice rischio di incorrere nelle sanzioni delle autorità UE per la protezione dei dati se non rispettano la pertinente normativa europea, e delle autorità USA se non rispettano quella americana.

³ Legge Sarbanes-Oxley, sezione 301(4).

⁴ La sezione 406 SOX e più in particolare i regolamenti attuati dalle principali Borse valori americane (NASDAQ, NYSE) stabiliscono anche che le società quotate su quei mercati debbano adottare "codici di condotta" che si applichino agli amministratori delegati e ai direttori finanziari, per quanto riguarda le questioni di contabilità, reporting e revisione contabile, corredati di meccanismi attuativi.

⁵ Norma 4350 (D) (3): "Responsabilità e autorità del comitato per la revisione dei conti"

⁶ New York Stock Exchange (NYSE), sezione 303A.06: "Comitato per la revisione dei conti"

L'applicabilità di alcune disposizioni della legge SOX alle controllate europee di società statunitensi e alle società europee quotate negli USA è attualmente all'esame delle autorità giurisdizionali americane⁷. Malgrado questa relativa incertezza sull'applicabilità integrale della SOX alle società stabilite in Europa, le imprese che sono ad essa soggette in virtù di chiare disposizioni extraterritoriali da quella previste vogliono potersi conformare anch'esse alle sue specifiche disposizioni sulla denuncia degli illeciti.

Dato il rischio di sanzioni cui sono esposte le imprese dell'UE, il Gruppo ex articolo 29 crede urgente incentrare la propria analisi essenzialmente sui sistemi di denuncia predisposti per segnalare eventuali violazioni riguardanti la contabilità, i controlli contabili interni e la revisione contabile di cui alla legge Sarbanes-Oxley, e sugli aspetti connessi che seguono. In questo modo il Gruppo intende contribuire a rafforzare la certezza del diritto delle imprese che soggiacciono nel contempo alle norme UE sulla protezione dei dati e alla legge SOX.

III. ENFASI PARTICOLARE POSTA DALLA NORME SULLA PROTEZIONE DEI DATI SULLA PROTEZIONE DELLA PERSONA DENUNCIATA

Le procedure interne per la denuncia delle irregolarità sono di norma improntate alla necessità di introdurre principi di buon governo societario nel funzionamento quotidiano delle imprese. La denuncia delle irregolarità si pone come meccanismo aggiuntivo affinché i dipendenti possano segnalare presunte violazioni per via interna, avvalendosi di uno specifico canale. Tale meccanismo integra i normali circuiti di informazione e reporting dell'organizzazione: rappresentanti dei lavoratori, gerarchia, responsabili del controllo della qualità o revisori interni, la cui funzione è per l'appunto quella di segnalare eventuali violazioni dell'etica di comportamento. La denuncia delle irregolarità dovrebbe quindi integrare, non già sostituire, la gestione interna.

Il Gruppo evidenzia la necessità di attuare procedure di denuncia in conformità delle norme europee sulla protezione dei dati. L'attuazione di tali procedure poggerà infatti, nella maggior parte dei casi, sul trattamento di dati personali (raccolta, registrazione, conservazione, comunicazione e distruzione di dati relativi a una persona fisica identificata o identificabile); pertanto, si applicano le norme sulla protezione dei dati.

L'applicazione di tali norme avrà conseguenze diverse sull'assetto e sulla gestione delle procedure in questione. La sezione IV illustra nel dettaglio l'intera gamma di queste conseguenze.

Il Gruppo osserva che le regole e gli orientamenti esistenti in materia di denuncia delle irregolarità sono diretti a proteggere soprattutto la persona che fa ricorso alle procedure di denuncia ("denunciante") e non fanno riferimento alcuno alla protezione del soggetto denunciato, né al trattamento dei suoi dati personali. Eppure chiunque gode, anche se accusato, dei diritti sanciti dalla direttiva 95/46/CE e dalle corrispondenti disposizioni di diritto interno.

⁷ La *US Court of Appeals (1st Circuit)* ha statuito il 5 gennaio 2006 che le disposizioni SOX sulla protezione del denunciante non si applicano ai cittadini stranieri che lavorano al di fuori degli USA per controllate straniere di società soggette alle altre disposizioni di quella legge.

Applicare le norme UE sulla protezione dei dati alle procedure di denuncia significa attribuire una specifica attenzione alla tutela della persona oggetto della segnalazione. Al riguardo, il Gruppo sottolinea che tali procedure comportano per la persona in questione un rischio assai grave di stigmatizzazione e vittimizzazione all'interno dell'organizzazione per cui lavora; un rischio al quale sarà esposta ancor prima di venire a conoscenza della denuncia che la riguarda e ancor prima che sia avviato il processo di verifica che ne determini la fondatezza.

Il Gruppo ritiene che una corretta applicazione delle norme sulla protezione dei dati alle procedure per la denuncia delle irregolarità contribuirà a contenere il margine di rischio. Non solo: lungi dall'impedire a queste procedure di funzionare secondo la loro intrinseca finalità, l'applicazione di tali norme contribuirà in linea generale al loro buon funzionamento.

IV. COMPATIBILITÀ DELLE PROCEDURE DI DENUNCIA CON LE NORME SULLA PROTEZIONE DEI DATI

Applicare le norme sulla protezione dei dati alle procedure di denuncia implica l'esame dei seguenti aspetti: legittimità dei sistemi di denuncia (1); applicazione dei principi relativi alla qualità dei dati e di proporzionalità (2); obbligo di fornire informazioni chiare e complete sulla procedura (3); diritti del soggetto denunciato (4); sicurezza dei trattamenti (5); gestione delle procedure interne di denuncia (6); aspetti connessi con il trasferimento internazionale dei dati (7); obbligo di notificazione e controllo preliminare (8).

1. *Legittimità dei sistemi di denuncia (articolo 7 della direttiva 95/46/CE)*

Una procedura interna di denuncia delle irregolarità è lecita se è lecito il trattamento dei dati personali e se ricorre una delle condizioni di cui all'articolo 7 della direttiva sulla protezione dei dati.

Allo stato attuale, due condizioni sembrano pertinenti in questo contesto: è necessario istituire un sistema interno di denuncia per adempiere un obbligo legale (articolo 7, lettera c)), oppure per perseguire l'interesse legittimo del responsabile del trattamento o dei terzi cui vengono comunicati i dati (articolo 7, lettera f))⁸.

i) Il sistema di denuncia è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento (articolo 7, lettera c))

L'istituzione di sistemi di segnalazione deve essere finalizzata a onorare un obbligo legale imposto dal diritto comunitario o dal diritto degli Stati membri, più in particolare un obbligo legale diretto a istituire procedure di controllo interno in settori specifici.

⁸ Le società dovrebbero sapere che in alcuni Stati membri il trattamento dei dati relativi a presunti reati penali è subordinato a ulteriori condizioni specifiche afferenti alla legittimità del loro trattamento (vedi *infra*, sezione IV, 8).

Al momento, tale obbligo sussiste in molti Stati membri dell'UE nel settore bancario per esempio, dacché i governi hanno deciso di rafforzarne il controllo interno, specie in relazione alle attività delle imprese d'investimento e degli enti creditizi.

L'obbligo legale di introdurre meccanismi di controllo rafforzati sussiste anche nel contesto della lotta alla corruzione, specie per effetto dell'attuazione nel diritto nazionale della convenzione OCSE sulla lotta alla corruzione dei funzionari pubblici stranieri nelle transazioni commerciali internazionali (convenzione OCSE del 17 dicembre 1997).

Al contrario, l'obbligo ai sensi di una legge o di un regolamento straniero di istituire sistemi di segnalazione non può configurare un obbligo legale in forza del quale sarebbe legittimo il trattamento dei dati nell'UE. Qualunque altra interpretazione permetterebbe a normative straniere di eludere facilmente le norme UE prescritte dalla direttiva 95/46/CE. Di conseguenza, le disposizioni della legge SOX sulla denuncia delle irregolarità non possono legittimare il trattamento di dati personali in base all'articolo 7, lettera c).

Tuttavia, in certi paesi dell'UE la necessità di istituire procedure di denuncia potrebbe discendere da obblighi giuridici vigenti ai sensi del diritto nazionale negli stessi settori contemplati dalla legge SOX⁹. In altri paesi dell'UE in cui tali obblighi giuridici non esistono, è tuttavia possibile raggiungere lo stesso scopo avvalendosi dell'articolo 7, lettera f).

ii) Il sistema di denuncia è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento (articolo 7, lettera f))

Istituire sistemi di segnalazione può essere necessario per perseguire l'interesse legittimo del responsabile del trattamento o dei terzi cui vengono comunicati i dati (articolo 7, lettera f)). Tale condizione sarebbe accettabile soltanto se su tale interesse legittimo “non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata”.

Le principali organizzazioni internazionali, fra cui l'UE¹⁰ e l'OCSE¹¹, hanno riconosciuto l'importanza dei principi di buon governo societario per garantire il corretto funzionamento delle organizzazioni. I principi e gli orientamenti elaborati in queste sedi promuovono la trasparenza, lo sviluppo di pratiche finanziarie e contabili sane per proteggere gli interessi degli azionisti e garantire una maggiore stabilità finanziaria dei mercati. In particolare, è riconosciuto l'interesse di ogni organizzazione a istituire procedure appropriate che permettano ai dipendenti di segnalare presunte irregolarità e pratiche contabili o di revisione censurabili al consiglio di amministrazione o al collegio dei sindaci. Tali procedure devono garantire che siano predisposti strumenti per lo svolgimento di indagini indipendenti e proporzionate sui fatti segnalati, ivi compresa un'adeguata procedura di selezione delle persone incaricate della gestione del sistema, e che vi siano i seguiti opportuni.

⁹ Codice olandese sul governo societario del 9.12.2003, sezione II, 1.6
Progetto spagnolo di codice unico sul governo societario delle imprese quotate, capitolo IV, 67(1)d). Il progetto è tuttora all'esame del garante spagnolo della protezione dei dati che ne sta valutando le implicazioni in termini di protezione dei dati.

¹⁰ Comunità europea: Raccomandazione della Commissione, del 15 febbraio 2005, sul ruolo degli amministratori senza incarichi esecutivi o dei membri del consiglio di sorveglianza delle società quotate e sui comitati del consiglio d'amministrazione o di sorveglianza (GU L 52 del 25.2.2005, pag. 51).

¹¹ OCSE: Principi OCSE sul governo societario. 2004. Parte I, sezione IV.

Inoltre, questi orientamenti e regolamenti evidenziano la necessità di garantire la protezione del denunciante e di predisporre le opportune garanzie per proteggerlo contro forme di ritorsione (provvedimenti discriminatori o disciplinari)¹².

In effetti, l'obiettivo di garantire la sicurezza finanziaria dei mercati finanziari internazionali, di prevenire in particolare la frode e comportamenti impropri in relazione alla tenuta della contabilità, ai controlli contabili interni, alla revisione contabile e al reporting, e di lottare contro la corruzione, la criminalità bancaria e finanziaria e l'abuso di informazioni privilegiate (*insider trading*) sembra costituire un interesse legittimo del datore di lavoro che giustifica il trattamento di dati personali nell'ambito dei sistemi interni di denuncia in quei settori. È nell'interesse precipuo di una società ad azionariato diffuso, specie se quotata in borsa, garantire che le segnalazioni di presunte manipolazioni contabili o di revisioni contabili errate, che potrebbero avere ripercussioni sul bilancio della società e intaccare l'interesse legittimo degli azionisti alla sua stabilità finanziaria, pervengano effettivamente al consiglio di amministrazione per un seguito adeguato.

In questo contesto, si può annoverare la legge statunitense Sarbanes-Oxley fra le iniziative assunte al fine di garantire la stabilità dei mercati finanziari e la protezione degli interessi legittimi degli aventi causa fissando regole finalizzate a garantire il buon governo societario.

Per tutti questi motivi, il Gruppo ritiene che, nei paesi dell'UE in cui non sussiste l'obbligo giuridico specifico di istituire procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria, i responsabili del trattamento dei dati hanno pur sempre un interesse legittimo nell'attuare tali sistemi interni nei settori indicati.

Ciò nondimeno, secondo l'articolo 7, lettera f) è necessario bilanciare l'interesse legittimo perseguito nel trattare i dati personali con i diritti fondamentali dell'interessato. Tale verifica del bilanciamento degli interessi dovrebbe tener conto di aspetti quali la proporzionalità, la sussidiarietà, la gravità delle presunte violazioni che è possibile segnalare, e le conseguenze per gli interessati. Ai fini di tale verifica sarà altresì necessario predisporre garanzie adeguate. In particolare, l'articolo 14 della direttiva 95/46/CE stabilisce che, nei casi in cui il trattamento si fonda sull'articolo 7, lettera f), l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi preminenti e legittimi, al trattamento di dati che lo riguardano. Segue una disamina di questi aspetti.

2. *Applicazione del principio relativo alla qualità dei dati e del principio di proporzionalità (articolo 6 della direttiva sulla protezione dei dati)*

Ai sensi della direttiva 95/46/CE i dati personali devono essere trattati lealmente e lecitamente¹³, rilevati per finalità determinate, esplicite e legittime¹⁴, e successivamente trattati in modo non incompatibile con tali finalità. Inoltre, i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o

¹² Si veda, per esempio, il *Public Interest Disclosure Act* britannico del 1998 (legge sulla divulgazione nell'interesse generale).

¹³ Articolo 6, paragrafo 1, lettera a) della direttiva 95/46/CE.

¹⁴ Articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE.

per le quali vengono successivamente trattati¹⁵. Combinate insieme, queste norme costituiscono il cosiddetto "principio di proporzionalità". Per finire, devono essere prese misure adeguate affinché siano cancellati o rettificati i dati inesatti o incompleti¹⁶. Dall'applicazione di queste norme essenziali deriva una serie di conseguenze sia per il modo in cui i dipendenti possono effettuare le segnalazioni, sia per il loro trattamento da parte dell'organizzazione. Segue un'analisi di queste conseguenze.

i) Possibile limitazione del numero di soggetti autorizzati a denunciare presunte irregolarità o violazioni dell'etica di comportamento

Conformemente al principio di proporzionalità, il Gruppo raccomanda che la società responsabile delle procedure interne di denuncia valuti attentamente se sia opportuno limitare il numero dei soggetti autorizzati a esperire quelle procedure per segnalare eventuali violazioni, specie alla luce della loro gravità. Il Gruppo ammette tuttavia la possibilità che in alcuni casi le categorie di personale elencate comprendano tutti i dipendenti per alcuni dei settori contemplati dal presente parere.

Le circostanze di ciascun caso assumeranno un valore decisivo, e il Gruppo ne è consapevole. Per questo non intende emettere un parere prescrittivo al riguardo ma lascia ai responsabili del trattamento, previa eventuale verifica delle autorità competenti, il compito di determinare se tali restrizioni siano appropriate nelle circostanze specifiche in cui operano.

ii) Possibile limitazione del numero di soggetti denunciabili

Conformemente al principio di proporzionalità, il Gruppo raccomanda che la società responsabile delle procedure interne di denuncia valuti attentamente se sia opportuno limitare il numero dei soggetti che è possibile segnalare con procedura di denuncia, specie alla luce della gravità delle violazioni segnalate. Il Gruppo ammette tuttavia la possibilità che in alcuni casi le categorie di personale elencate comprendano tutti i dipendenti per alcuni dei settori contemplati dal presente parere.

Le circostanze di ciascun caso assumeranno un valore decisivo, e il Gruppo ne è consapevole. Per questo non intende emettere un parere prescrittivo al riguardo ma lascia ai responsabili del trattamento, previa eventuale verifica delle autorità competenti, il compito di determinare se tali restrizioni siano appropriate nelle circostanze specifiche in cui operano.

iii) Promozione delle denunce nominative e riservate rispetto alle denunce anonime

Se le procedure interne di denuncia debbano permettere di effettuare segnalazioni anonime anziché in forma nominativa (ossia con individuazione dell'autore, e comunque in regime di riservatezza) è questione che merita un'attenzione specifica.

L'anonimato può non essere una buona soluzione, sia per il denunciante sia per l'organizzazione, e questo per una serie di motivi:

- l'anonimato non garantisce che altri non riescano a indovinare chi ha denunciato il problema;

¹⁵ Articolo 6, paragrafo 1, lettera c) della direttiva 95/46/CE.

¹⁶ Articolo 6, paragrafo 1, lettera d) della direttiva 95/46/CE.

- è più difficile verificare la fondatezza della denuncia se non è possibile fare altre domande per approfondire la questione;
- è più facile organizzare la protezione del denunciante contro eventuali ritorsioni, specie se tale protezione è prevista per legge¹⁷, quando il problema è denunciato apertamente;
- le denunce anonime possono concentrare l'attenzione sul denunciante, magari per il sospetto che abbia denunciato il problema in malafede;
- l'organizzazione corre il rischio di alimentare una cultura della delazione;
- il clima sociale dell'organizzazione potrebbe deteriorarsi se i dipendenti sanno di poter essere denunciati su base anonima in un qualsiasi momento.

Rispetto alle norme sulla protezione dei dati, le denunce anonime creano un problema specifico che attiene al requisito essenziale per cui i dati personali devono essere rilevati lealmente. In linea di massima, il Gruppo reputa che solo le segnalazioni nominative debbano essere trasmesse attraverso procedure interne di denuncia per soddisfare questo requisito.

Il Gruppo si rende conto, tuttavia, che non sempre il denunciante ha la possibilità o la predisposizione psicologica necessaria per presentare una segnalazione nominativa. Sa anche che le denunce anonime sono una realtà nel mondo societario, anche e soprattutto qualora manchino sistemi di denuncia riservati e strutturati, e che non è possibile ignorare tale realtà. Il Gruppo ritiene quindi che le procedure per la denuncia di irregolarità possano dar luogo a denunce anonime e ai successivi provvedimenti, ma che ciò debba costituire un'eccezione e rispondere alle seguenti condizioni.

Il Gruppo ritiene che le procedure interne di denuncia debbano essere concepite in modo da non incoraggiare la delazione anonima come mezzo ordinario per segnalare un'irregolarità. In particolare, le imprese non dovrebbero richiamare l'attenzione sulla possibilità di presentare segnalazioni anonime attraverso tali procedure. Al contrario, poiché queste ultime dovrebbero garantire la riservatezza del trattamento dei dati relativi all'identità del denunciante, colui che intenda segnalare un'irregolarità mediante un sistema di denuncia deve sapere che non dovrà temere le conseguenze della sua azione. Perciò è necessario che il denunciante sia informato, sin dal momento in cui entra in contatto con il sistema, che questo ne garantisce la riservatezza in tutti gli stadi del procedimento e, in particolare, che la sua identità non sarà rivelata a terzi, siano questi il denunciato o i superiori gerarchici. Se, nonostante tale informativa, colui che avvia la procedura vuole restare comunque anonimo, la denuncia sarà accettata nel sistema. Il denunciante deve inoltre sapere che potrebbe essere necessario svelarne l'identità ai soggetti competenti che parteciperanno alle indagini o ai procedimenti giudiziari successivi, iniziati a seguito della verifica svolta nell'ambito della procedura di denuncia.

Il trattamento delle denunce anonime deve essere oggetto di speciali precauzioni. Sarebbe opportuno, per esempio, che il primo destinatario della denuncia ne esamini l'ammissibilità e valuti se sia opportuno farla circolare nel sistema. Potrebbe inoltre essere utile valutare se sia preferibile verificare e trattare le denunce anonime più rapidamente rispetto alle denunce riservate, a causa del rischio di abusi. L'opportunità di adottare speciali precauzioni non significa, tuttavia, che le denunce anonime non debbano essere verificate con la dovuta attenzione per tutti i fatti in causa, al pari delle denunce nominative.

¹⁷ Per esempio, a norma del *Public Interest Disclosure Act* britannico.

iv) Proporzionalità e esattezza dei dati rilevati e trattati

Ai sensi dell'articolo 6, paragrafo 1, lettere b) e c), della direttiva sulla protezione dei dati, i dati personali devono essere rilevati per finalità determinate, esplicite e legittime e devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati.

Poiché l'obiettivo del sistema di segnalazione è garantire il buon governo societario, i dati rilevati e trattati nell'ambito delle procedure di denuncia delle irregolarità dovrebbero riguardare esclusivamente i fatti connessi con quella finalità. Le società che introducono tali procedure dovrebbero definire chiaramente il tipo di informazioni divulgabili nel sistema, limitandole a quanto attiene alla tenuta della contabilità, ai controlli contabili interni, alla revisione contabile, alla lotta contro la corruzione e alla criminalità bancaria e finanziaria. È cosa ammessa che in alcuni paesi la legge può disporre espressamente che le procedure interne di denuncia si applichino anche ad altre categorie di gravi illeciti, la cui divulgazione può essere necessaria nell'interesse generale¹⁸, tuttavia queste non rientrano nell'oggetto del presente parere; potrebbero in effetti non applicarsi in altri paesi. I dati personali trattati nell'ambito della procedura dovrebbero limitarsi a quelli strettamente e obiettivamente necessari per verificare la fondatezza della denuncia. È inoltre opportuno che le denunce siano tenute separate dagli altri dati personali.

I fatti segnalati nell'ambito di una procedura di denuncia che non abbiano attinenza con i settori oggetto della stessa potrebbero essere trasmessi a funzionari competenti della società/organizzazione se è in gioco l'interesse vitale dell'interessato o l'integrità morale dei dipendenti, ovvero se il diritto nazionale fa obbligo di comunicare quell'informativa agli organi o alle autorità pubbliche che esercitano l'azione penale.

v) Osservanza dei termini di conservazione dei dati

La direttiva 95/46/CE stabilisce che i dati personali devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Tale requisito è essenziale per garantire l'osservanza del principio di proporzionalità del trattamento.

I dati personali trattati nell'ambito di una procedura interna di denuncia dovrebbero essere cancellati prontamente e di norma entro due mesi dal completamento della verifica dei fatti esposti nella denuncia.

Tale termine sarebbe diverso in caso di azione giudiziaria o disciplinare nei confronti del denunciato o del denunciante che avesse reso dichiarazioni false o diffamatorie. I dati personali dovrebbero allora essere conservati fino a conclusione del procedimento ed allo spirare dei termini per proporre impugnazione. I termini di conservazione saranno stabiliti dalla legislazione dei singoli Stati membri.

I dati personali afferenti a segnalazioni che l'autorità incaricata del trattamento giudica infondate dovrebbero essere cancellati senza indugio.

¹⁸ Per esempio, il *Public Interest Disclosure Act* britannico del 1998.

Restano inoltre d'applicazione eventuali normative nazionali in materia di archiviazione dei dati nella società. Queste potranno in particolare autorizzare l'accesso ai dati conservati negli archivi e specificare le finalità per cui è consentito, le categorie di soggetti autorizzati e altre norme eventuali in materia di sicurezza.

3. *Informativa chiara e completa sulla procedura (articolo 10 della direttiva sulla protezione dei dati)*

L'obbligo di fornire informazioni chiare e complete sul sistema impone al responsabile del trattamento di informare l'interessato sull'esistenza, le finalità e il funzionamento del sistema, sui destinatari delle denunce e sul diritto di accesso, rettifica e cancellazione riconosciuto alla persona denunciata.

Il responsabile del trattamento deve altresì comunicare che sarà garantita la riservatezza del denunciante per l'intero procedimento e che l'uso illegale del sistema può comportare provvedimenti nei confronti dell'autore dell'abuso. D'altro canto, può essere anche notificato agli utenti del sistema che non incorreranno in sanzioni se ne faranno uso in buona fede.

4. *Diritti del denunciato*

Il quadro giuridico istituito dalla direttiva 95/46/CE evidenzia in modo specifico la protezione dei dati personali dell'interessato. Di conseguenza, stando a tale quadro le procedure interne di denuncia dovrebbero incentrarsi sui diritti dell'interessato, fermi restando quelli del denunciante. Occorre quindi trovare un punto di bilanciamento degli interessi fra i diritti di tutte le parti interessate, comprese le esigenze legittime dell'impresa con riguardo alle azioni di verifica.

i) Diritti di informazione

L'articolo 11 della direttiva 95/46/CE dispone l'obbligo di informare l'interessato in caso di dati raccolti presso terzi e non già presso l'interessato stesso.

Il responsabile della procedura dovrà informare il denunciato quanto prima materialmente possibile dacché vengono registrati i dati che lo riguardano. Secondo l'articolo 14, l'interessato ha anche il diritto di opporsi al trattamento dei suoi dati personali se questo è legittimato dall'articolo 7, lettera f). Tuttavia, tale diritto di opposizione è esercitabile soltanto per motivi preminenti e legittimi, derivanti dalla situazione specifica della persona interessata.

In particolare, al dipendente denunciato devono essere notificati: [1] l'identità del responsabile della procedura interna di denuncia, [2] i fatti di cui è accusato, [3] i dipartimenti o servizi dell'impresa o delle altre entità o imprese del gruppo cui quella appartiene ai quali può pervenire la denuncia e [4] le modalità per esercitare il diritto di accesso ai dati e di rettifica.

Se invece esiste il rischio sostanziale che comunicando tali informazioni si comprometta la capacità dell'impresa di verificare efficacemente la fondatezza della denuncia o di raccogliere le prove necessarie, la notifica all'interessato potrà essere ritardata fintanto che sussiste questo rischio. Tale eccezione alla norma di cui all'articolo 11 è intesa a proteggere le prove, evitandone la distruzione o l'alterazione da parte del denunciato, va applicata in maniera restrittiva, caso per caso, e deve tener conto dei più ampi interessi in gioco.

La procedura di denuncia deve contemplare i dispositivi necessari per impedire la distruzione delle informazioni divulgate.

ii) Diritto di accesso, di rettifica e di cancellazione

L'articolo 12 della direttiva 95/46/CE riconosce all'interessato la facoltà di accedere ai dati registrati che lo riguardano per verificarne l'esattezza e rettificarli se inesatti, incompleti o non aggiornati (diritto di accesso e di rettifica). Nel predisporre un sistema di segnalazione occorre pertanto assicurare che sia rispettato il diritto di accesso e di rettifica dei dati inesatti, incompleti o non aggiornati.

Tuttavia, l'esercizio di tale diritto può essere limitato per garantire la tutela di diritti e libertà altrui nell'ambito del sistema. Tale limitazione va applicata caso per caso.

In nessuna circostanza può essere permesso al denunciato di avvalersi del suo diritto di accesso per ottenere informazioni sull'identità del denunciante, salvo se il denunciante ha dichiarato il falso in malafede. In tutti gli altri casi, dovrà essere sempre garantita la riservatezza dei dati sull'identità del denunciante.

Inoltre, l'interessato ha il diritto di rettificare o cancellare i dati che lo riguardano se il trattamento non è conforme alle disposizioni della direttiva, in particolare a causa del carattere incompleto o inesatto dei dati (articolo 12, lettera b)).

5. *Sicurezza dei trattamenti (articolo 17 della direttiva 95/46/CE)*

i) Misure di sicurezza pertinenti

L'articolo 17 della direttiva 95/46/CE fa obbligo alla società o organizzazione responsabile delle procedure interne di denuncia di prendere tutte le precauzioni tecniche e organizzative ragionevoli per tutelare la sicurezza dei dati raccolti, diffusi o conservati. L'obiettivo è garantire la protezione dei dati dalla distruzione accidentale o illecita, dalla perdita accidentale, dalla diffusione o dall'accesso non autorizzati.

Le segnalazioni possono essere raccolte con qualunque strumento di trattamento dei dati, elettronico o no. Tale strumento deve essere riservato al sistema di denuncia onde prevenirne l'impiego per scopi diversi da quello cui era destinato e per una maggiore riservatezza dei dati.

Queste misure di sicurezza devono essere commisurate allo scopo di verificare i fatti denunciati, in conformità con le regole di sicurezza in vigore nei diversi Stati membri.

Nei casi in cui il sistema di denuncia sia gestito da un fornitore esterno, il responsabile del trattamento dei dati deve disporre di un contratto che ne certifichi l'adeguatezza e, soprattutto, deve prendere tutti i provvedimenti del caso per garantire la sicurezza delle informazioni trattate nell'intero procedimento.

ii) Riservatezza delle segnalazioni effettuate attraverso procedure interne di denuncia

La riservatezza delle denunce è una condizione essenziale per onorare l'obbligo imposto dalla direttiva 95/46/CE di garantire la sicurezza dei trattamenti.

Per raggiungere gli scopi cui è destinata una procedura per la denuncia delle irregolarità e incoraggiarne l'uso per segnalare fatti che configurino violazioni dell'etica di comportamento o la commissione di illeciti all'interno dell'impresa, è essenziale proteggere adeguatamente l'autore della segnalazione, garantendo la riservatezza di quest'ultima e impedendo a terzi di scoprire l'identità dell'autore.

Le imprese che istituiscono procedure interne di denuncia devono provvedere affinché l'identità del denunciante resti segreta e non sia comunicata al denunciato durante le attività di verifica. Tuttavia, se viene accertata l'infondatezza di una denuncia e la malafede del denunciante, è possibile che il denunciato voglia avviare un procedimento per diffamazione e che sia quindi necessario rivelargli l'identità del denunciante, se il diritto nazionale lo consente. Le leggi e i principi di diritto nazionale sulla denuncia delle irregolarità in relazione al governo societario dispongono che i dipendenti che segnalano violazioni non debbano essere soggetti ad alcuna forma di ritorsione, come provvedimenti discriminatori o disciplinari irrogati dall'impresa o dall'organizzazione.

La riservatezza dei dati personali deve essere garantita ogni qualvolta questi siano rilevati, comunicati o memorizzati.

6. *Gestione delle procedure di denuncia*

Le procedure di denuncia presuppongono che si esaminino attentamente le modalità per la raccolta e la gestione delle denunce. Il gruppo, pur prediligendo la gestione interna del sistema, ammette tuttavia che un'impresa possa decidere di avvalersi di fornitori esterni cui affidare parte di tale gestione, soprattutto la raccolta delle segnalazioni. I fornitori esterni devono essere vincolati dall'obbligo rigoroso della riservatezza e impegnarsi a rispettare i principi di protezione dei dati. Indipendentemente dal sistema che avrà attuato, un'impresa dovrà conformarsi in particolare agli articoli 16 e 17 della direttiva.

i) Organizzazione specifica interna della gestione delle procedure di denuncia

All'interno dell'impresa o del gruppo deve essere istituito un organo specifico preposto alla gestione delle denunce e all'attività di verifica.

L'organo preposto deve comporsi di personale ad hoc in possesso di una specifica formazione, limitato nel numero e vincolato per contratto da obblighi di riservatezza specifici.

Il sistema di denuncia deve essere rigorosamente separato dagli altri dipartimenti della società, come il dipartimento Risorse Umane.

Sarà suo compito provvedere affinché le informazioni raccolte e trattate siano trasmesse, per quanto necessario, solo e soltanto ai funzionari specificamente competenti, all'interno dell'impresa o del gruppo cui quella appartiene, ad avviare il procedimento di verifica o ad adottare le misure necessarie in funzione delle risultanze. I destinatari delle informazioni dispongono affinché queste ultime siano gestite in regime di riservatezza e siano applicate le dovute misure di sicurezza.

ii) Possibilità di ricorrere a fornitori esterni

Le imprese o i gruppi di imprese che affidano a fornitori esterni parte della gestione del sistema di denuncia restano responsabili delle operazioni di trattamento che ne risultano in quanto i fornitori esterni operano unicamente in qualità di incaricati del trattamento ai sensi della direttiva 95/46/CE.

I fornitori esterni possono essere imprese che gestiscono call center ovvero imprese o studi legali specializzati nel raccogliere le denunce e incaricati talvolta di svolgere parte delle necessarie attività di verifica.

Tali fornitori esterni dovranno conformarsi ai principi della direttiva 95/46/CE e provvedere, in forza di un contratto con l'impresa per conto della quale gestiscono il sistema, a rilevare e trattare le informazioni secondo i principi della richiamata direttiva e a trattare le informazioni soltanto per gli scopi specifici per cui sono state raccolte. In particolare, dovranno rispettare l'obbligo di riservatezza e comunicare le informazioni trattate solo e soltanto ai funzionari specificamente competenti, all'interno dell'impresa o del gruppo cui quella appartiene, ad avviare il procedimento di verifica o ad adottare le misure necessarie in funzione delle risultanze. Si conformeranno inoltre ai termini di conservazione che vincolano il responsabile del trattamento. L'impresa che si avvale di tali meccanismi, in qualità di responsabile del trattamento, è tenuta a verificare periodicamente l'ottemperanza dei fornitori esterni ai principi della direttiva.

iii) Principio di verifica nell'UE per le imprese europee e eccezioni

La natura e la struttura stessa delle multinazionali comportano che possa essere necessario diffondere l'oggetto e gli esiti di una denuncia in tutto il gruppo di imprese, anche fuori dell'Unione.

Secondo il principio di proporzionalità, dovrebbero essere la natura e la gravità dell'illecito, in linea di principio, a determinare a quale livello, e quindi in quale paese, debba situarsi la valutazione della denuncia. In linea di massima, il Gruppo ex articolo 29 ritiene che la verifica dovrebbe svolgersi a livello locale, ossia in un paese dell'UE, e che l'informazione non dovrebbe essere automaticamente condivisa con le altre imprese della multinazionale.

Il Gruppo riconosce tuttavia l'esistenza di alcune eccezioni a questa regola.

I dati ricevuti nell'ambito del sistema di denuncia possono essere comunicati all'interno del gruppo se tale comunicazione è necessaria ai fini della verifica, in funzione della natura e della gravità della presunta violazione, o se risulta dalla composizione stessa del gruppo. La comunicazione sarà necessaria ai fini della verifica se, per esempio, la denuncia riguarda un partner di un'altra persona giuridica appartenente al gruppo, un esponente di livello o un manager dell'impresa interessata. In questo caso, i dati devono essere comunicati soltanto in condizioni di riservatezza e di sicurezza all'organo competente della persona giuridica destinataria, che predispone garanzie equivalenti per quanto riguarda la gestione delle procedure di denuncia in qualità di organizzazione preposta a gestire le denunce nell'impresa dell'UE.

7. *Trasferimenti verso paesi terzi*

Quando dati personali sono trasferiti verso paesi terzi si applicano gli articoli 25 e 26 della direttiva 95/46/CE. Le disposizioni di tali articoli si applicano in particolare quando l'impresa ha affidato parte della gestione del sistema di denuncia a fornitori terzi stabiliti fuori dell'Unione, o quando i dati raccolti nelle denunce sono fatti circolare all'interno del gruppo, pervenendo quindi anche a imprese situate fuori dell'UE.

Tali trasferimenti sono particolarmente probabili con riguardo alle controllate UE di imprese di paesi terzi.

Quando il paese terzo cui saranno trasmessi i dati non garantisce un livello di protezione adeguato ai sensi dell'articolo 25 della direttiva 95/46/CE, i dati potranno essere trasmessi alle seguenti condizioni:

[1] il destinatario dei dati personali è un soggetto stabilito negli USA che aderisce all'accordo *Safe Harbor* (approdo sicuro);

[2] il destinatario ha sottoscritto con l'impresa UE che trasferisce i dati un contratto di trasferimento in virtù del quale l'impresa presenta garanzie sufficienti, in base per esempio alle clausole contrattuali tipo pubblicate dalla Commissione europea nelle sue decisioni del 15 giugno 2001 e del 27 dicembre 2004;

[3] il destinatario attua un corpus di norme vincolanti di governo societario che le autorità competenti per la protezione dei dati hanno debitamente approvato.

8. *Adempimento degli obblighi di notificazione*

In conformità degli articoli da 18 a 20 della direttiva sulla protezione dei dati, le imprese che introducono procedure interne per la denuncia di irregolarità devono adempiere agli obblighi di notificazione e/o controllo preliminare nei confronti delle autorità nazionali di protezione dei dati.

Negli Stati membri in cui vige tale procedura, potrebbero essere oggetto di controllo preliminare a cura dell'autorità nazionale di protezione dei dati i trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone. Ciò potrebbe verificarsi nell'ipotesi in cui il diritto nazionale consenta il trattamento dei dati relativi a presunti reati di persone giuridiche private a certe condizioni, compreso il controllo preliminare dell'autorità competente per la protezione dei dati. Oppure, nell'eventualità in cui l'autorità nazionale ritenga che il trattamento possa privare il denunciato di un diritto, di un beneficio o un contratto. Spetta al diritto nazionale e alla pratica dell'autorità nazionale di protezione dei dati valutare se i trattamenti in questione debbano essere oggetto di controllo preliminare.

V – CONCLUSIONI

Il Gruppo riconosce che le procedure interne di denuncia possono rappresentare un meccanismo utile con cui le imprese o le organizzazioni possono monitorare l'osservanza di norme e disposizioni di governo societario, specie in relazione alla tenuta della contabilità, ai controlli contabili interni e alla revisione contabile, le disposizioni in materia di lotta contro la corruzione, la criminalità bancaria e finanziaria e il diritto penale. Esse possono aiutare un'impresa a attuare correttamente i principi di governo societario e a individuare i fatti che ne comprometterebbero la posizione.

Il Gruppo sottolinea la necessità che le procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria, oggetto del presente parere, siano attuate nel rispetto dei principi di protezione dei dati personali sanciti dalla direttiva 95/46/CE. L'osservanza di tali principi contribuisce infatti al corretto funzionamento del sistema ad opera delle imprese e delle stesse procedure di denuncia. È in effetti essenziale che nell'attuare una procedura interna di denuncia sia garantito il diritto fondamentale alla protezione dei dati personali, sia del denunciante che del denunciato, per l'intero procedimento.

Il Gruppo ex articolo 29 ribadisce che i principi di protezione dei dati dettati dalla direttiva 95/46/CE debbano applicarsi integralmente alle procedure interne di denuncia, specie per quanto attiene al diritto del denunciato di essere informato, di accedere ai dati che lo riguardano, di chiederne la rettifica e la cancellazione. Tuttavia, visti i diversi interessi in gioco, il Gruppo riconosce che l'esercizio di questi diritti può essere soggetto a limitazioni in casi assai specifici, in un'ottica di bilanciamento fra il diritto alla privacy e gli interessi del sistema. Tali limitazioni dovranno tuttavia applicarsi in modo restrittivo, nella misura in cui siano necessarie al raggiungimento degli obiettivi del sistema.

Bruxelles, 1° febbraio 2006

Per il Gruppo

Il Presidente
Peter Schaar