

POSSIBILE RUOLO DEI *WHISTLEBLOWING* SCHEMES NEL CONTESTO DELLA *CORPORATE* E DELLA *CONTROL GOVERNANCE*. PROFILI DI COMPATIBILITA' CON L'ORDINAMENTO ITALIANO E, IN PARTICOLARE, CON LA DISCIPLINA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Avv. Matteo Bascelli, Avvocato in Milano

1. Premessa

Lo spunto per le considerazioni che seguono è offerto, nello specifico, dalla pubblicazione del cd. "WP117" ossia il "Parere 1/2006 sull'applicazione della disciplina comunitaria in materia di protezione dei dati personali alle procedure informative implementate nei settori attinenti l'attività contabile e dei controlli interni, della revisione, nonché della lotta alla corruzione ed ai crimini bancari e finanziari"¹, adottato in data 1 febbraio 2006 dal cd. "Gruppo di lavoro sulla protezione dei dati personali - Art. 29"².

¹ Il titolo in lingua inglese del "WP117" è "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime", il cui testo integrale è consultabile sul sito web http://europa.eu.int/comm/justice_home/fsj/privacy/. Alla data in cui il presente contributo è stato consegnato per la stampa, l'unica autorità nazionale che risulta essersi compiutamente pronunciata in materia di compatibilità dei *dispositifs d'alerte professionnelle* (o *whistleblowing schemes*) rispetto all'ordinamento giuridico di appartenenza, risulta essere stata la francese *Commission nationale de l'informatique et des libertés* ("CNIL"), con l'emanazione della *Délibération n. 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle*, consultabile sul sito della stessa autorità www.cnil.fr, alla quale si farà cenno nel prosieguo. Il tema in esame risulta altresì essere oggetto di analisi da parte della lussemburghese *Commission nationale pour la protection des données* (www.cnpd.lu) e da parte dell'olandese *Dutch Data Protection Authority* (www.dutchdpa.nl). Prende atto dell'esistenza del "fenomeno del *whistleblowing*" anche il Garante per la protezione dei dati personali italiano, nell'ambito della propria Relazione 2005, p. 150, offrendone, tuttavia, una definizione che appare limitata ("segnalazioni anonime effettuate da dipendenti di un'azienda attraverso linee dedicate, cd. *integrity lines*") e nella successiva Relazione 2006, p. 151, ove è dato atto dell'esistenza del WP117. Nessun riferimento diretto è presente, invece, nel documento del Garante italiano dedicato alle "Linee Guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" del 23 novembre 2006, né nel Provvedimento a carattere generale del medesimo Garante emanato in data 1 marzo 2007 dal titolo "Lavoro: le Linee Guida del Garante per posta elettronica e *internet*".

² Il "Gruppo di lavoro" è stato costituito in applicazione dell'art. 29 direttiva 95/46/CE, in quanto organismo europeo indipendente con finalità consultive che si occupa di protezione dei dati e di riservatezza. I suoi compiti sono descritti nell'art. 30 direttiva 95/46/CE e nell'art. 15 direttiva 2002/58/CE.

La finalità espressa del Parere WP117 è quella di offrire alle persone giuridiche interessate idonee Linee Guida in merito alla corretta adozione ed attuazione al proprio interno dei cd. *whistleblowing schemes* (traducibile, meno efficacemente, in “procedure di segnalazione di comportamenti illeciti”), alla luce dell’applicazione della disciplina comunitaria in materia di protezione dei dati personali, contenuta principalmente nella direttiva 95/46/CE del 24 ottobre 1995³.

In un’ottica di più ampio respiro, l’analisi dei *whistleblowing schemes* offre lo spunto per riflettere, pur se solo incidentalmente, sulla sempre più marcata tendenza dell’ordinamento italiano di indurre e, talvolta, imporre alle società - in particolar modo quelle quotate - l’adozione di sistemi di *corporate* e di *control governance* a carattere prevalentemente endogeno, in quanto promossi, gestiti e fatti funzionare all’interno e dall’interno delle società stesse. Tale tendenza risulta essere spesso frutto, come si avrà modo di accennare, delle spinte di una politica economica comunitaria la quale, consapevole del fenomeno della globalizzazione economica e finanziaria a livello mondiale, tende ad una sempre maggiore integrazione del sistema europeo, con il fine di potenziarne la concorrenzialità. E’ infatti opinione condivisa che un solido sistema di *corporate governance* - inteso come insieme di procedure, soggetti e norme, giuridiche e tecniche, finalizzate ad assicurare un governo d’impresa efficiente e corretto nei confronti di tutti i soggetti interessati alla vita dell’impresa stessa - massimizzi il valore delle società e consenta di raggiungere un livello di competitività in grado di garantire la capacità di attrazione delle scelte degli investitori⁴.

Quali manifestazioni concrete dell’evoluzione di cui sopra possono essere citati, a mero titolo esemplificativo, a livello nazionale, i codici di autodisciplina (tra i quali il Codice di Autodisciplina delle Società Quotate di Borsa Italiana SpA), i codici di condotta o di comportamento (ai quali fa ora riferimento l’art. 124-bis d.lgs. 58/1998, sulla scorta del *comply or explain approach*), le procedure di disciplina sugli abusi di mercato (con particolare riferimento a quelle attinenti all’*internal dealing* ai sensi degli artt. 152-bis ss. del Regolamento Emittenti di CONSOB), i Modelli di Organizzazione e di Gestione idonei a prevenire la realizzazione degli illeciti penali (di cui al d.lgs. 231/2001), sino ad arrivare, più nello specifico, ai sistemi di controlli interni volti a prevenire situazioni di conflitto di interessi nel settore del risparmio gestito (a seguito della direttiva 2004/39/CE, come modificata dalla direttiva

³ Si ricorda che l’Italia ha attuato la direttiva 95/46/CE con la legge 31 dicembre 1996, n. 675 (“Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”), successivamente abrogata e sostituita dal d.lgs. 30 giugno 2003, n. 196 (“Codice in materia di protezione dei dati personali”).

⁴ A conferma della molteplicità degli interessi la cui tutela può essere garantita dall’adozione di validi principi di *corporate governance*, la risoluzione adottata dall’ETUC (*European Trade Union Confederation*) a Bruxelles il 14-15 marzo 2006, così si esprime: “*EU company law initiatives should therefore endorse the emergence and evolution of a European model of corporate governance, fostering company boards’ orientation towards long-term value creation, high-trust labour relations, workers’ participation in companies’ decision-making processes and societal responsibility. Not only shareholders, but also workers, other citizens and the community at large have an interest in good corporate governance. Accordingly, the European corporate governance framework should lay down proper institutional conditions for companies to promote long-term profitability and employment prospects, define mechanisms that prevent mismanagement and guarantee transparency and accountability with regard to investments and their returns*”. Un’interessante analisi in merito al fenomeno del *whistleblowing* quale “oggetto di studio da parte di diverse discipline, che ne hanno approfondito aspetti di carattere etico, sociale, psicologico, giuridico ed aziendale organizzativo, inserendolo nell’ambito delle aree tematiche della gestione delle risorse umane, del controllo (interno ed esterno) e, più in generale, della *corporate governance*”, è offerto da C. FLORIO, *Il whistleblowing nella letteratura internazionale: aspetti definitivi e fattori determinanti*, in *Rivista dei dottori commercialisti*, 2007, n. 5, p. 927.

2006/31/CE, conosciuta anche come MiFID - *Markets in Financial Instruments Directive* e delle relative misure di esecuzione rappresentate dalla direttiva 2006/73/CE e dal regolamento CE n. 1286/2006⁵.

A tali procedure si accompagnano peraltro, in numero proporzionalmente crescente, nuovi organi di controllo, interni o esterni alle società (comitati endo-consiliari per la remunerazione, per la nomina e per il controllo interno, soggetti preposti alla funzione di *internal audit*, Organismi di Vigilanza, ecc.), specificamente addetti alla loro attuazione, gestione e funzionamento, il cui fine ultimo dovrebbe consistere nell'aumento di efficienza del lavoro svolto dagli organi societari tradizionalmente deputati alle funzioni di gestione e controllo⁶.

L'aumento esponenziale delle suddette procedure e dei relativi organi presenta - al fianco degli attesi benefici in termini di maggiore trasparenza, partecipazione e consapevolezza generale dell'agire societario - aspetti problematici relativi al necessario coordinamento di attività tra i medesimi ed impone in alcuni casi, come per i *whistleblowing schemes* dei quali più direttamente ci si occuperà, preventive analisi di compatibilità con l'ordinamento nazionale.

2. I *whistleblowing schemes*

Aiuta a comprendere meglio l'esigenza sottesa alla finalità propria del Parere WP117, e lo scopo della presente analisi, chiarire che per *whistleblowing schemes* s'intendono quelle procedure di cui si dotano le società, private o pubbliche, per dare modo al personale dipendente (ma non solo) di segnalare ad Organismi di Vigilanza interni o esterni, secondo modalità predeterminate, la conoscenza di comportamenti censurabili, in quanto contrari a disposizioni normative o a regolamenti aziendali (*wrongdoing*), compiuti da altri soggetti all'interno delle stesse società. Tali procedure sono quindi finalizzate ad essere di valido ausilio per una corretta applicazione dei principi di *corporate* e, più specificamente, di *control governance*, nell'ambito della quotidiana attività societaria. Esse, come già scritto, forniscono infatti un efficace supporto alle funzioni interne aziendali classicamente deputate ad attività di *reporting* a beneficio dei vertici aziendali (società di revisione, comitati di controllo interno, ufficio del personale, controllo della qualità, ecc.)⁷.

⁵ Evidenzia come tra gli strumenti di intervento che hanno permesso al sistema di *corporate governance* di evolversi debbano segnalarsi, oltre alle riforme normative organiche tra le quali quella sulle società di capitali del 2003, i codici di autodisciplina, i codici etici, i codici di comportamento e, in generale, i sistemi di controllo endosocietari, M. CARDIA, *Codice di autodisciplina e normativa 231*, in *La responsabilità amministrativa delle società e degli enti*, n. 3, luglio-settembre 2006, pp. 63 ss..

⁶ In tal senso si esprime la Raccomandazione della Commissione Europea 2005/162/CE 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.

⁷ Per una puntuale analisi dell'impatto che l'introduzione dei Modelli Organizzativi assimilabili a quelli in esame ha sulla *corporate governance* societaria, si rimanda, tra gli altri, a D. GALLETTI, *I Modelli Organizzativi nel d.lgs. 231/2001: le implicazioni per la corporate governance*, disponibile sul sito *web* dell'Università di Trento, www.jus.univr.it, nonché A. ALESSANDRI, *Corporate governance nelle società quotate: riflessi penalistici e nuovi reati societari*, in *Giur. comm.*, 2002, 5, pp. 547 ss.. Per un'approfondita descrizione degli elementi costitutivi e procedurali dei *whistleblowing schemes*, si veda C. FLORIO, *op. cit.*, p. 929, ove pure è posto bene in evidenza come questo tipo di comunicazioni "contro-corrente" o *upstream* - in quanto dirette "dai livelli inferiori della piramide organizzativa per raggiungere i livelli superiori" - siano idonee a contribuire al buon funzionamento dei sistemi di controllo interno. Tale funzione è oramai riconosciuta dai

Se quelle sopra tratteggiate risultano essere le legittime finalità sottese a detti schemi endosocietari, risulta tuttavia di immediata evidenza come l'adozione di tale tipo di procedure comporti un'inevitabile "invasione" di sfere giuridiche altrui, anche queste oggetto di tutela da parte dell'ordinamento, con eguale intensità e pur spesso di opposta direzione.

Ai limitati fini che più direttamente attengono alla presente analisi, si pensi a quanto inscindibile sia il momento funzionale di detti schemi rispetto al "trattamento" (inteso ai sensi dell'art. 1, comma 1, lett. a), d.lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali") che consegue alla raccolta, registrazione, conservazione, elaborazione, comunicazione e, infine, distruzione delle ingenti quantità di dati personali relativi non solo al soggetto segnalante (*whistleblower*), ma anche al soggetto segnalato⁸.

La contrapposizione tra interessi egualmente degni di tutela (riservatezza, da un lato, e tutela dell'integrità aziendale, dall'altro) insita nell'esplicarsi delle procedure in esame⁹ è destinata peraltro ad acuirsi ed arricchirsi di nuove problematiche laddove il comportamento censurabile sia attribuibile non ad altro dipendente, ma alla società stessa (nelle persone dei suoi esponenti aziendali apicali) presso la quale il *whistleblower* presta la propria attività lavorativa. In tali ultime fattispecie, infatti, entra altresì in gioco il delicato bilanciamento tra l'interesse al decoro e all'immagine della struttura aziendale, per un verso, e il diritto di critica e di denuncia del dipendente che renda pubbliche situazioni produttive a rischio o disfunzioni organizzative, per altro verso¹⁰. Palese emerge dunque il dilemma generato dal sistema che, attraverso

massimi organismi internazionali nella definizione dei principi di controllo quali il *Committee of Sponsoring Organizations of the Treadway Commission* (CoSO), il cui *CoSO Report* del 1992 è ancor oggi indicato come *best practice* di riferimento per l'architettura dei sistemi di controllo interno dal *Sarbanes-Oxley Act*. Sul tema, si veda anche il pregevole contributo di G. FERRARINI, *Controlli interni e strutture di governo societario*, in *Il nuovo diritto delle società*, Liber amicorum Gian Franco Campobasso, a cura di P. ABBADESSA-G.B. PORTALE, Utet, 2006, vol. 3, IX.

⁸ Sembra cogliere gli "assai delicati problemi di confidenzialità delle informazioni" oggetto di trattamento nella fase di funzionamento dei Modelli in esame, G. CAPECCHI, *La responsabilità amministrativa degli enti per gli illeciti amministrativi dipendenti da reato: note di inquadramento sistematico e problematiche operative*, in *Diritto del commercio internazionale*, 20.1 - gennaio-marzo 2006, p. 111, e, in particolare, p. 117, ove si fa presente l'istituzione, invalsa nella prassi societaria statunitense, di canali riservati di informazione (cd. *bolines*) tramite i quali è consentito ai dipendenti che intendano denunciare una violazione del codice di condotta aziendale di procedere con segnalazioni anonime.

⁹ La questione della contrapposizione di interessi in ambiente lavorativo è affrontata nelle Linee Guida proposte dal cd. "WP55" ossia il "Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro" adottato il 29 maggio 2002 dal Gruppo di lavoro sulla protezione dei dati. - Art. 29 (ad integrazione del cd. "WP 48" ossia il "Parere 8/2001 sul trattamento di dati personali in ambito lavorativo", adottato dal medesimo Gruppo di lavoro il 13 settembre 2001), la cui finalità espressa è quella di "offrire indirizzi interpretativi ed esempi concreti circa quanto costituisce attività legittima di controllo e circa i limiti accettabili della vigilanza sui dipendenti". La difficoltà alla quale si fa riferimento è lucidamente espressa nel Parere sopra menzionato, nel quale si legge: "Quando al mattino si recano a lavorare i lavoratori non abbandonano fuori dell'ufficio o della fabbrica i loro diritti alla riservatezza ed alla protezione dei dati. Essi possono legittimamente attendersi di usufruire di un certo grado di riservatezza sul posto di lavoro, visto che una parte significativa delle loro relazioni con altri esseri umani si sviluppa nell'ambiente di lavoro. Questo diritto è tuttavia controbilanciato da altri diritti ed interessi legittimi del datore di lavoro; quest'ultimo ha in particolare il diritto di gestire la sua azienda con una certa efficienza, ma soprattutto il diritto di tutelarsi contro le responsabilità od i danni cui possono dare origine gli atti dei lavoratori. Questi diritti ed interessi costituiscono motivi legittimi atti a giustificare opportuni provvedimenti volti a limitare i diritti del dipendente alla riservatezza. A questi effetti l'esempio più chiaro è dato dai casi in cui il datore di lavoro è vittima di un atto perseguibile penalmente del dipendente".

¹⁰ L'individuazione del confine che il dipendente non deve oltrepassare nell'esprimere valutazioni critiche con riferimento all'operato del proprio datore di lavoro, al fine di non incorrere in sanzioni disciplinari anche per aver contravenuto al disposto dell'art. 2105 c.c., può essere rilevato in alcune pronunce giurisprudenziali in tema di obbligo di fedeltà del dipendente e suo diritto di critica. Il riferimento è a Cass., Sez. Lav., 14 giugno 2004, n. 11220 (in *Orientamenti della giurisprudenza del lavoro*, 2004, pp. 410 ss., e in *Massimario della giurisprudenza del lavoro*, novembre 2004, n. 11, pp. 813 ss., con nota di V. NUZZO), e a Cass., Sez. Lav., 16 maggio 1998, n. 4952 (in *Rivista giuridica del lavoro e della previdenza sociale*, 1999, pp. 455 ss., con nota di M. AIMO, ove l'autrice dedica un'accurata analisi alla figura del *whistleblower*).

differenti e contrapposti gruppi di norme settoriali, persegue la tutela di valori (o interessi) per loro natura antinomici.

Il Gruppo di lavoro si è mosso nella consapevolezza che l'adozione ed attuazione dei *whistleblowing schemes* può far sorgere in ciascuno dei Paesi membri dell'UE numerose problematiche, verosimilmente differenti tra loro, in ragione delle diverse impostazioni culturali ancora sensibili nell'Unione Europea. Prova ne è - come si scriverà in seguito - che in alcuni Paesi membri i *whistleblowing schemes* sono previsti per legge, mentre in altri è del tutto assente qualsiasi normativa in materia.

Alla luce di quanto precede, il Gruppo di lavoro, alla ricerca di un ideale quanto arduo punto di bilanciamento di interessi, ha inteso emanare un parere non definitivo, ma "interlocutorio", limitato, peraltro, ai soli settori attinenti l'attività contabile e dei controlli interni, della revisione, nonché della lotta alla corruzione ed ai crimini bancari e finanziari, riservandosi di intervenire successivamente in ulteriori ambiti, quali quelli delle risorse umane, della sicurezza e salute sul posto di lavoro e dei danni ambientali. Approccio, questo, che, come si chiarirà in appresso e pur su di un piano parzialmente diverso, ricorda da vicino quello adottato dal legislatore italiano nell'introduzione nell'ordinamento nazionale della "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", con il d.lgs. 8 giugno 2001, n. 231.

In particolare, il Gruppo di lavoro si è sentito chiamato ad un urgente intervento interpretativo avendo a mente le concrete difficoltà che alcuni gruppi societari multinazionali stanno affrontando sin dall'introduzione della *Sarbanes-Oxley Act* ("SOX"), adottata dal Congresso degli Stati Uniti d'America nel 2002, al fine di porre tempestivo rimedio ai noti scandali finanziari ivi accaduti. Tali difficoltà derivano dalla circostanza che la SOX, così come i relativi regolamenti applicativi di Borsa del Nasdaq e del NYSE, impongono alle società quotate statunitensi ed alle loro controllate con sede in Europa, a pena di pesanti sanzioni, di adottare all'interno dei rispettivi comitati di controllo (o *audit committee*) procedure idonee a consentire ai dipendenti di presentare, su base confidenziale ed anonima, rilievi in relazione a questioni contabili, di revisione o di controllo.

Quale conseguenza dell'incertezza circa la compatibilità dei *whistleblowing schemes* con la disciplina comunitaria in materia di protezione di dati personali, i suddetti gruppi societari con sedi sia negli USA, che in Stati membri UE, si trovano attualmente nell'"imbarazzo" di dover scegliere se rischiare sanzioni irrogate dalle autorità di vigilanza europee, per non aver ottemperato alle prescrizioni dettate (ad esempio, ma non solo) in materia di protezione di dati personali nell'attuazione delle menzionate procedure informative, ovvero se rischiare sanzioni dalle autorità di vigilanza di mercato statunitensi, per non aver compiutamente adottato le procedure a presidio degli obblighi informativi previsti nella SOX¹¹. Si tratta, com'è facilmente

¹¹ E' interessante notare che l'applicazione della disciplina comunitaria in materia di protezione dei dati personali ha già fatto emergere in passato contrasti, non ancora del tutto risolti, tra l'Unione Europea e gli USA. La decisione n. 2000/520/CE del 26 luglio 2000 rappresenta, infatti, un parziale e non poco sofferto tentativo di soluzione agli specifici problemi di trasferimenti di dati verso gli USA. L'accordo è stato adottato dopo tre anni di negoziato tra la Commissione Europea - rappresentata, tra gli altri, dal Commissario europeo per il mercato interno, Frits Bolkestein - e l'amministrazione Clinton - nella persona del funzionario del Ministero del commercio USA, David Aaron. Tale decisione prevede l'adesione volontaria delle imprese americane ad un sistema basato su un primo nucleo di principi tratti dalla direttiva europea 95/46/CE: informativa agli interessati; scelta (*opt-out*) per i dati non sensibili, anche per cessione a terzi; consenso (*opt-in*) per i dati sensibili; accesso ai dati; rettifica e, in casi eccezionali, cancellazione dei dati trattati; sicurezza delle

intuibile, di un'evidente manifestazione di quella antinomia di norme (nella fattispecie a livello sovranazionale) alla quale si è fatto cenno sopra.

3. Le Linee Guida fornite dal Parere WP117

Le Linee Guida fornite nel Parere WP117 sono chiaramente ed inevitabilmente ispirate agli ormai consolidati principi di necessità, finalità, trasparenza, legittimità, proporzionalità ed accuratezza, che sono alla base dell'intera disciplina in materia di protezione dei dati personali e che risultano necessari al fine di poter correttamente esperire quel delicato processo che consiste nel bilanciamento di interessi (o *balance of interest test*) rappresentati, da un lato, dal diritto di ciascun individuo alla protezione dei dati personali¹² e, dall'altro, da una serie astrattamente infinita di interessi, che spesso appaiono opposti o inconciliabili rispetto al primo, tra i quali emergono quelli intimamente legati al diritto di libera iniziativa economica ed ai connessi strumenti di tutela.

Tali principi si traducono, nella fattispecie, in una verifica di compatibilità dei *whistleblowing schemes* con: (i) la rispettiva fonte legittimante; (ii) la "qualità" e la proporzionalità dei dati trattati; (iii) la "trasparenza" nell'adozione e nell'applicazione delle procedure; (iv) il rispetto dei diritti dei soggetti segnalati; (v) la sicurezza dei sistemi di trattamento dei dati; (vi) la corretta gestione delle procedure; (vii) il rispetto delle regole poste in merito al trasferimento all'estero dei dati trattati; (viii) l'obbligo di notifica e di controllo da parte delle autorità di vigilanza competenti.

Considerata l'importanza di detti principi, nonché l'autorevolezza in materia del Gruppo di lavoro¹³, se ne intende offrire di seguito una sintetica descrizione, secondo quanto espresso nel Parere in esame.

informazioni; loro pertinenza rispetto agli scopi per i quali sono raccolte. Tali cautele consentirebbero alle imprese che esportano dati negli USA di non esporsi ad interventi europei di blocco di trasferimenti di dati, così come prevede la direttiva europea in caso di non adeguata protezione. In caso di reclamo, è previsto che le persone possano rivolgersi a organismi privati di risoluzione delle controversie (ad esempio, *BBB online*), nonché alla *Federal Trade Commission* o al Ministero dei trasporti USA (per le compagnie aeree). Sulla specifica problematica USA-UE in materia di *whistleblowing schemes* risulta di interesse l'intervento effettuato presso l'*Annual Meeting 2006* dell'*American Bar Association* tenutosi ad Honolulu (HI) nei giorni 5-8 agosto 2006, da T. GILLOT, *Whistleblowing and codes of conduct in Europe - The difficult implementation of SOX whistleblower provisions in France*, consultabile al seguente indirizzo internet: <http://www.bna.com/bnabooks/ababna/annual/2006/10.pdf>.

¹² L'espressione "protezione dei dati personali", affermata dall'art. 1 d.lgs. 196/2003, può sinteticamente essere descritta come il diritto dell'individuo a vedersi assicurato un adeguato livello di tutela dei diritti e delle libertà fondamentali, nonché della dignità dello stesso, con particolare riferimento alla riservatezza e all'identità personale (art. 2, comma 1, d.lgs. 196/2003).

¹³ Si ricorda che, pur avendo il Gruppo di lavoro compiti consultivi, esso è composto, tra gli altri, da un rappresentante delle autorità di controllo designate da ciascuno Stato membro UE. Tale (parziale) identità soggettiva tra ente sovranazionale e autorità garante nazionale lascerebbe intendere una condivisione di approccio alle problematiche in parola e, quindi, un verosimile pronunciamento di quest'ultima secondo le Linee Guida già espresse nel Parere WP117. Un'eventuale decisione in tal senso da parte del Garante per la protezione dei dati personali potrebbe avere un effetto immediato sui titolari di trattamenti, in ragione del potere riconosciuto alla citata autorità dall'art. 154, comma 1, lett. c), d.lgs. 196/2003. Sulla sempre più immanente presenza delle autorità amministrative cd. "indipendenti" attraverso l'incessante opera di regolamentazione delle attività svolte nei settori di competenza e dei connessi poteri di soluzione delle controversie, la letteratura è vasta. La funzione di "giudici del comportamento dell'operatore economico" delle autorità indipendenti, le cui "decisioni sono destinate a divenire orientamenti per la valutazione della correttezza dei soggetti che operano nel settore di mercato da esse regolato", è evidenziata da G. VETTORI, *Le asimmetrie informative fra regole di validità e regole di responsabilità*, in *Rivista di diritto privato*, n. 2/2003, Milano, pp. 253 ss.. Dei poteri normativi e di quelli "paragiurisdizionali" delle autorità amministrative scrive M. ORLANDI, *Autonomia privata e autorità indipendenti*, in *Rivista di diritto privato*, n. 2/2003, Milano, pp. 271 ss..

(i) Fonte legittimante

Al fine di verificare la liceità dell'adozione, dell'attuazione e del funzionamento dei *whistleblowing schemes*, è in primo luogo necessario verificare se il trattamento dei dati personali che ne consegue rientri in una delle ipotesi legittimanti previste dall'art. 7 direttiva 95/46/CE e, in particolare, se esso sia necessario: (i) per adempiere ad un obbligo di legge al quale il titolare del trattamento è tenuto; ovvero (ii) per il perseguimento di un interesse legittimo del titolare del trattamento ovvero di soggetti terzi ai quali i dati sono comunicati, sempreché, in tale seconda ipotesi, non risultino prevalenti i diritti e le libertà fondamentali dell'interessato, in ossequio al principio di bilanciamento di interessi appena menzionato.

Quanto alla prima ipotesi legittimante, nel Parere WP117 si dà atto della circostanza che in alcuni Paesi membri dell'Unione Europea esistono leggi che prevedono l'attuazione di procedure idonee a consentire l'effettuazione di controlli interni alla stregua dei *whistleblowing schemes*, soprattutto con riferimento al settore bancario e nelle attività di contrasto alla corruzione¹⁴. Il riferimento è, in particolare, al recepimento della Convenzione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) del 17 dicembre 1997, avente ad oggetto la "Lotta contro la corruzione dei pubblici funzionari nelle transazioni internazionali", di cui è stato di recente celebrato a Roma, in data 21 novembre 2007, il decimo anniversario con la firma dell'"Impegno comune" da parte dei 30 Paesi membri OCSE (oltre a 7 Paesi non OCSE).

Si ricorda che la previsione della responsabilità amministrativa delle società per determinate fattispecie di reato era contenuta nell'art. 2 della suddetta Convenzione OCSE. Tale tipo di responsabilità è stato successivamente introdotto nell'ordinamento italiano dall'art. 11 legge 29 settembre 2000, n. 300, di ratifica ed esecuzione delle Convenzioni OCSE e Unione Europea contro la corruzione nel commercio internazionale e contro la frode ai danni della Comunità Europea. Il d.lgs. 231/2001 rappresenta, appunto, l'attuazione del Governo italiano della delega ad esso attribuita dal suddetto art. 11, legge 300/2000, a disciplinare l'articolazione di questo tipo di responsabilità¹⁵.

Come già anticipato, ove non ricorra l'ipotesi dell'applicazione dei *whistleblowing schemes* in forza di una previsione normativa, è pur sempre possibile verificarne la liceità alla luce della loro idoneità a tutelare un interesse legittimo del titolare del trattamento ovvero di soggetti terzi ai quali i dati sono comunicati. In tale circostanza, tuttavia, sarà sempre necessario verificare che non risultino prevalenti i diritti e le libertà fondamentali dei soggetti potenzialmente coinvolti, chiamando così

¹⁴ Tra i pochi Paesi UE dotati di una normativa specifica in tale settore, vi è il Regno Unito il cui *Public Interest Disclosure Act* del 1998, in vigore dal 2 luglio 1999, "*applies to people at work raising genuine concerns about crime, civil offences (including negligence, breach of contract, breach of administrative law), miscarriage of justice, danger to health and safety or the environment and the cover up of any of these. It applies whether or not the information is confidential and extends to malpractice occurring overseas*". Offre un efficace panorama, anche internazionale, delle questioni connesse all'utilizzo dei *whistleblowing schemes* il sito *web* dell'autorità indipendente britannica denominata *Public Concern at Work* ("PCaW") (www.pcaw.co.uk).

¹⁵ Per un'ampia analisi dello stato di attuazione in Italia della citata Convenzione, si consiglia la lettura del "*Report on the application of the convention on combating bribery of foreign public officials in international business transactions and the 1997 recommendation on combating bribery in international business transactions*", approvato ed adottato dal cd. *Working Group on Bribery in International Business Transactions* il 29 novembre 2004, consultabile sul sito *web* www.oecd.org, ove ampio spazio è dedicato all'applicazione in Italia del d.lgs. 231/2001. Un panorama aggiornato sul punto lo offrono i diversi contributi pubblicati su *Guida al Diritto, Diritto Comunitario e Internazionale*, n. 1, gennaio-febbraio 2008, pp. 9 ss..

nuovamente in causa quella delicata valutazione di bilanciamento degli interessi alla quale abbiamo accennato.

A tale proposito, il Parere fa riferimento alla circostanza che l'Unione Europea e, ancora una volta, l'OCSE, hanno riconosciuto l'importanza che l'adozione di idonee regole di *corporate governance* atte ad assicurare un elevato livello di trasparenza e correttezza nelle pratiche attinenti il settore finanziario e amministrativo in generale, hanno sulla protezione degli *stakeholders* e sulla solidità dell'intero sistema economico¹⁶. E, tra i richiamati principi e Linee Guida di *corporate governance*, rientrano certamente le procedure che consentono ai dipendenti di riferire direttamente ai comitati di controllo e di sorveglianza la conoscenza di comportamenti illegali o semplicemente censurabili rispetto a regole di condotta stabilite a tutela dell'integrità del patrimonio aziendale.

Così scrivendo, il Gruppo di lavoro riconosce astrattamente all'obiettivo di assicurare solidità finanziaria ai mercati internazionali, anche attraverso l'implementazione di procedure atte a contrastare efficacemente all'interno delle società comportamenti fraudolenti e criminosi, un valore di per sé tale da consentire l'operazione di bilanciamento di interessi di cui sopra.

Alla luce di quanto precede, sembrerebbe potersi sin d'ora affermare che l'adozione di *whistleblowing schemes*, ove rispettosi delle condizioni di cui in appresso, possa considerarsi legittimata non tanto in ragione di una specifica fonte normativa (considerati i più ristretti ambiti applicativi, sia soggettivo che oggettivo, del d.lgs. 231/2001), quanto piuttosto dall'identità di *ratio* sottesa, individuabile, come scritto, nella tutela del sistema economico nell'ambito del quale lo stesso soggetto giuridico chiamato all'attuazione di detti schemi opera.

(ii) Qualità e proporzionalità dei dati trattati

La direttiva 95/46/CE prescrive all'art. 6, comma 1 (recepito dall'art. 11 d.lgs. 196/2003), che i dati personali siano trattati in modo leale e lecito, raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità. I dati personali debbono altresì risultare adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati, devono essere esatti e, se necessario, aggiornati e devono essere conservati in modo tale da consentire l'identificazione delle persone interessate per un periodo di tempo non superiore a quello necessario per il perseguimento delle finalità di raccolta.

Le suddette prescrizioni sono sintetizzabili nei concetti di "qualità" e "proporzionalità" dei dati e rappresentano preziose indicazioni circa le caratteristiche che qualsiasi *whistleblowing scheme* deve avere al fine di risultare rispettoso dei principi posti a tutela dei dati personali oggetto di trattamento.

Il Gruppo di lavoro offre quindi all'interprete alcune "chiavi di lettura", oltremodo interessanti sul piano operativo, nell'implementazione dei *whistleblowing schemes*, sintetizzabili nell'elenco che segue:

¹⁶ Il riferimento è, rispettivamente, alla già citata Raccomandazione della Commissione Europea 2005/162/CE e al Documento OECD - *Principles of Corporate Governance* del 2004.

- risulta opportuno verificare se sia preferibile limitare il novero dei soggetti che possono avere accesso al *whistleblowing scheme* in qualità di *whistleblowers*, individuandoli preventivamente in ragione delle loro specifiche funzioni e posizioni aziendali;
- dovrebbe essere valutato se sia preferibile limitare il novero dei soggetti che possono essere segnalati attraverso i *whistleblowing schemes*, anche in tal caso individuandoli preventivamente in ragione delle loro specifiche funzioni e posizioni aziendali;
- appare preferibile limitare l'accesso ai *whistleblowing schemes* tramite segnalazioni non anonime, sebbene effettuate su base strettamente confidenziale, considerando che, da un lato, l'anonimato non risulta idoneo a meglio proteggere il *whistleblower* rispetto ad eventuali ritorsioni e, dall'altro, che maggiore risulterebbe il rischio di segnalazioni fraudolentemente infondate. Sul punto, il Gruppo di lavoro, consapevole che vi possono essere soggetti i quali, pur a conoscenza di comportamenti illeciti, non provvedano a segnalarli per timore di essere "scoperti", ammette l'*anonymous complaints*, ma solo come eccezione alla regola dell'*identified reports*. Al fine di non incoraggiare l'anonimato, il Gruppo di lavoro pone l'accento sulla circostanza che nell'implementare i *whistleblowing schemes* le società informino il personale dipendente dell'elevato livello di confidenzialità con il quale saranno trattati i dati raccolti e che l'identità del *whistleblower* non sarà resa nota né al soggetto segnalato, né ai rispettivi superiori gerarchici¹⁷. Il Gruppo di lavoro suggerisce, peraltro, che, in un'ottica di massima trasparenza, al *whistleblower* sia reso noto che la sua identità potrebbe essere comunicata alle persone che ne facciano richiesta nell'ambito di procedimenti giudiziari iniziati sulla base della segnalazione stessa. Eventuali segnalazioni anonime dovranno essere trattate con estrema cautela, dando, ad esempio, indicazioni al soggetto istituzionalmente incaricato di riceverle, di valutarne l'attendibilità prima di dar luogo agli accertamenti del caso;
- le società che implementino i *whistleblowing schemes* dovrebbero definire preventivamente e con chiarezza il tipo di informazioni che possono essere oggetto di segnalazione e che oggetto di trattamento siano solo ed esclusivamente le informazioni necessarie per l'effettuazione degli accertamenti strettamente connessi. Nel caso siano comunque riferite circostanze che esulano dai "confini" così prestabiliti, le informazioni raccolte potranno essere rese note ai competenti soggetti all'interno della società, solo ed unicamente nel caso in cui siano in gioco interessi primari dei soggetti potenzialmente coinvolti ovvero vi siano obblighi di legge in tal senso;
- infine, risulta opportuno che i *whistleblowing schemes* definiscano precise indicazioni in merito al periodo di conservazione dei dati raccolti, periodo che, secondo il Gruppo di lavoro, non dovrebbe mai eccedere i 2 mesi dalla conclusione delle indagini, salvo che contro il soggetto segnalato o contro il *whistleblower* siano iniziati procedimenti giudiziari. In tal caso, il termine massimo di conservazione sarà stabilito con riferimento alle leggi nazionali. All'opposto, i

¹⁷ In senso conforme, le citate "Linee Guida" di Confindustria, suggeriscono che "nel disciplinare un sistema di *reporting* efficace sarà opportuno garantire la riservatezza a chi segnala le violazioni. Allo stesso tempo, sarà opportuno prevedere misure deterrenti contro ogni informativa impropria, sia in termini di contenuti che di forma".

dati raccolti dovranno essere immediatamente distrutti nel caso in cui l'organismo preposto a ricevere le segnalazioni le ritenga palesemente infondate.

(iii) "Trasparenza" nell'adozione e nell'applicazione delle procedure

In ossequio all'art. 10 direttiva 95/46/CE (recepito dall'art. 13 d.lgs. 196/2003), il Gruppo di lavoro suggerisce che l'implementazione dei *whistleblowing schemes* sia accompagnata da un'adeguata, completa e chiara informativa da fornire ai soggetti potenzialmente interessati e che tale *disclosure* sia rivolta non solo alla loro esistenza, finalità e funzionamento (compresa l'individuazione dell'organismo incaricato della raccolta delle segnalazioni), ma rappresenti anche il diritto di accesso, rettifica e cancellazione dei dati raccolti.

L'informativa dovrà altresì fornire adeguate rassicurazioni circa la confidenzialità con la quale saranno trattate le informazioni raccolte e che l'utilizzo in buona fede dei *whistleblowing schemes* porrà il *whistleblower* al riparo da qualsiasi azione da parte della società¹⁸.

(iv) Diritti dei soggetti segnalati

L'adozione ed il funzionamento dei *whistleblowing schemes* dovrà altresì porre attenzione all'ulteriore delicata operazione di bilanciamento degli interessi, da svolgere, questa volta, tra il soggetto segnalante ed il soggetto segnalato.

In tale ottica, il soggetto segnalato dovrà essere informato dall'organismo preposto non appena concretamente possibile, successivamente alla raccolta dei dati che lo riguardano. Egli dovrà in particolare essere informato in merito all'organismo che ha in carica la segnalazione (soprattutto se la società ne ha organizzati più d'uno) e di quello/i che all'interno della società potranno riceverne notizia, i fatti per i quali è stato segnalato, nonché l'esistenza dei suoi diritti di accesso e rettifica e le modalità per esercitarli.

Soltanto ove si corra il concreto rischio che la suddetta informativa possa pregiudicare la possibilità da parte della società di investigare efficacemente sui fatti segnalati, questa potrà essere ritardata sino al perdurare di tale rischio. Considerata la gravità della compressione del diritto all'informativa, tale posticipazione potrà essere applicata solo in casi eccezionali, caso per caso, ove ricorra il serio rischio di distruzione o alterazione delle prove da parte del soggetto segnalato.

Quanto ai diritti di accesso e rettifica da parte del soggetto segnalato, anche a questo proposito, il Gruppo di lavoro ne ritiene possibile una compressione soltanto in casi eccezionali e da valutare caso per caso, ove i diritti e le libertà di altri soggetti possano risulterne pregiudicati.

¹⁸ In tal senso già si esprimono le "Linee Guida" di Confindustria, secondo le quali, se si parte dalla considerazione che sul prestatore di lavoro incombono precisi doveri di diligenza verso il datore di lavoro, alla stregua di quanto prescritto, ad esempio, dagli artt. 2104 e 2105 c.c., "rientrando in tali doveri, il corretto adempimento all'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari". Le rassicurazioni da offrire al *whistleblower* paiono particolarmente opportune alla luce delle pronunce giurisprudenziali in tema di obbligo di fedeltà del dipendente e suo diritto di critica, di cui sopra alla nota 10.

(v) Sicurezza dei sistemi di trattamento dei dati

Conformemente a quanto stabilito dall'art. 17 direttiva 95/46/CE (recepito dagli artt. 33 ss. d.lgs. 196/2003), i soggetti che adottino i *whistleblowing schemes* dovranno attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati.

Alla luce della suddetta fondamentale prescrizione, alle procedure in esame dovrà essere specificamente dedicato personale adeguatamente istruito che sia posto in grado di trattare i dati raccolti con strumenti che rispondano ai requisiti di sicurezza prescritti.

Il Gruppo di lavoro ritiene che il soggetto preposto alla ricezione delle segnalazioni e gestore dei *whistleblowing schemes* possa anche essere individuato all'esterno della società interessata, imponendo tuttavia, in tal caso, che il relativo rapporto sia appositamente disciplinato sulla base di un contratto che imponga in capo all'*outsourcer* livelli di sicurezza e confidenzialità almeno equivalenti a quelli che avrebbe dovuto assicurare la società al proprio interno¹⁹. Poiché tali strutture esterne (tra le quali il Gruppo di lavoro menziona società che gestiscono *call centres* o, addirittura, studi legali specializzati) dovranno rivestire la qualifica di *processors* (o "responsabili" del trattamento, secondo la qualificazione italiana di cui all'art. 29 d.lgs. 196/2003), sulle società graveranno in ogni caso le eventuali responsabilità per *culpa in eligendo* e/o *in vigilando*.

(vi) Gestione delle procedure

Sia che la società decida di gestire internamente i *whistleblowing schemes*, sia che ne esternalizzi la gestione, i soggetti preposti dovranno essere dotati, come già scritto, di una struttura adeguata per organizzazione e mezzi, specificamente istruiti e dedicati a tale funzione, nonché contrattualmente vincolati a severi obblighi di riservatezza e confidenzialità.

Il Gruppo di lavoro suggerisce che tali strutture siano del tutto autonome ed indipendenti rispetto al resto dell'organizzazione, alla stregua di quanto accade, ad esempio, per l'ufficio del personale. Tale struttura (interna o esterna che sia) avrà l'obbligo di riferire soltanto e direttamente ai soggetti interni alla società dotati del potere di assumere le decisioni del caso, anch'essi vincolati ad impegni di riservatezza e confidenzialità.

E' opportuno notare come tutte dette caratteristiche siano analoghe a quelle che si dirà devono essere proprie degli Organismi di Vigilanza di cui al d.lgs. 231/2001, come chiaramente enunciato nella relativa Relazione di accompagnamento.

¹⁹ A proposito dell'individuazione del soggetto preposto alla gestione dei *whistleblowing schemes*, si ricorda - per analogia di funzioni che qui pare lecito applicare - che la Relazione di accompagnamento al d.lgs. 231/2001 propende per una scelta "interna" alla società che decida di implementare il Modello di Organizzazione e di Gestione ai sensi della citata normativa. Anche in questo contesto sembra opportuno ricordare che nell'individuazione del/i soggetto/i che può/possono assumere la veste di "Organismo di Vigilanza" ai sensi dell'art. 6, comma 1, lett. b), d.lgs. 231/2001, le "Linee Guida" di Confindustria, dopo aver escluso - almeno per le realtà societarie di maggiori dimensioni - il consiglio d'amministrazione, il collegio sindacale, nonché le funzioni del personale ed organizzazione, del legale, dell'amministrazione e dei controlli gestionali, ritiene particolarmente idonea detta attribuzione di compiti e responsabilità alle "nuove" figure rappresentate dal "comitato per il controllo interno", dall'organismo dedicato all'attività di *internal auditing* ovvero, infine, da organismi costituiti *ad hoc*, con la presenza, ad esempio, di amministratori non esecutivi e/o indipendenti.

(vii) Trasferimento all'estero dei dati trattati

Poiché potrà accadere che i dati personali raccolti nell'ambito dei *whistleblowing schemes* debbano essere trasferiti verso Paesi non appartenenti all'Unione Europea, in ragione del fatto che l'*outsourcer* eventualmente preposto dalla società ivi abbia la sede, ovvero che dette informazioni debbano essere verificate e/o valutate all'interno di gruppi multinazionali, il Gruppo di lavoro si è soffermato sull'applicazione degli artt. 25 e 26 direttiva 95/46/CE (recepiti dagli artt. 42 ss. d.lgs. 196/2003).

In particolare, il Gruppo di lavoro ha evidenziato che nel caso in cui il Paese di destinazione non assicuri al trattamento dei dati personali trasferiti un livello di protezione "adeguato" (da valutarsi alla luce della natura dei dati, della finalità del trattamento, del Paese d'origine e del Paese di destinazione, delle norme di diritto, delle regole professionali e delle misure di sicurezza ivi vigenti), il trasferimento è possibile ai sensi dell'art. 26, comma 2 (non apparendo verosimile che nella fattispecie possano ricorrere le esenzioni di cui al comma 1, legate al consenso dell'interessato, all'esecuzione di un contratto, alla salvaguardia di un interesse pubblico rilevante o alla salvaguardia di un interesse vitale dell'interessato), soltanto ove: (i) il destinatario abbia sede negli USA ed abbia aderito al *Safe Harbor Scheme*; (ii) il destinatario abbia sottoscritto un contratto con la società mittente con sede nell'UE, tramite il quale presti garanzie sufficienti ad assicurare la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché l'esercizio dei diritti connessi; ovvero, infine (iii) il destinatario dimostri di essersi dotato di un *corpus* vincolante di regole che sia stato ritenuto adeguato dalle competenti autorità di vigilanza in materia di protezione dei dati personali.

(viii) Notifica e controllo da parte delle autorità di vigilanza competenti

Il Gruppo di lavoro è, infine, consapevole del fatto che l'implementazione dei *whistleblowing schemes* dovrà essere valutata nei singoli Paesi membri alla luce dell'eventuale obbligo di notifica alle o controllo preventivo da parte delle autorità di vigilanza in materia di protezione dei dati personali, alla stregua di quanto prescritto dagli artt. 18 e 20 direttiva 95/46/CE (recepiti dagli artt. 37 ss. d.lgs. 196/2003), rimettendo ai soggetti interessati una valutazione da effettuare, caso per caso, in base alle singole leggi nazionali di recepimento della direttiva.

4.1 Brevi cenni all'esperienza italiana dei Modelli societari di Organizzazione e di Gestione idonei a prevenire reati. Punti di contatto con i *whistleblowing schemes*

Prima di procedere nel tentativo di ipotizzare le modalità secondo le quali adottare e attuare *whistleblowing schemes* nell'ambito delle realtà societarie italiane, sia consentita una rapida digressione, facendo riferimento all'unica esperienza che l'ordinamento giuridico italiano ha sinora conosciuto con riguardo a veri e propri modelli di controllo di carattere endosocietario (diversi, ovviamente, da quelli propri degli organi societari tradizionalmente chiamati a svolgere le funzioni di controllo contabile).

E' infatti opportuno ricordare che alcuni dei tratti caratterizzanti le procedure di cui si discute non sono del tutto ignoti nel panorama normativo nazionale, avendovi fatto ingresso - come accennato in apertura - in applicazione dei generali principi di trasparenza e correttezza ai quali dev'essere sempre più informato l'agire societario.

Il già citato d.lgs. 231/2001 ha introdotto per la prima volta nell'ordinamento italiano la responsabilità in sede penale delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, che si aggiunge a quella della persona fisica che ha commesso il fatto illecito.

Come si legge nelle "Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex d.lgs. 231/2001" di Confindustria, elaborate a partire dal 2002 e definitivamente approvate dal Ministero della Giustizia nel giugno 2004 (in corso di aggiornamento), la *ratio* sottesa a tale novità normativa sta nel fatto che "l'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, i quali, fino all'entrata in vigore della legge in esame, non pativano conseguenze dalla realizzazione di reati commessi, con vantaggio della società, da amministratori e/o dipendenti", provocando con ciò "un interesse di quei soggetti (soci, associati, ecc.) che partecipano alle vicende patrimoniali dell'ente, al controllo della regolarità e della legalità dell'operato sociale".

La tipologia di reati cui si applica la disciplina in esame non costituisce un *numerus clausus* ed infatti alle fattispecie originariamente previste negli artt. 24 (*Indebita percezione di erogazioni pubbliche, truffa in danno dello Stato o di altro ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di altro ente pubblico*) e 25 (*Concussione e corruzione*) si è assistito nel corso degli anni - secondo quanto previsto nella Relazione di accompagnamento al d.lgs. 231/2001 - ad interventi normativi che hanno esteso il ventaglio dei reati cui si applica detta disciplina.

Si sono così aggiunti l'art. 25-*bis*, relativo alle falsità in monete, carte di pubblico credito e in valori di bollo; l'art. 25-*ter*, che ha esteso la responsabilità amministrativa ad alcune fattispecie di reati societari²⁰ commessi nell'interesse, ma non anche a vantaggio, della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità agli obblighi inerenti la loro carica. Sono stati altresì successivamente inseriti l'art. 25-*quater*, che stabilisce la responsabilità amministrativa dell'ente anche in relazione alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico; l'art. 25-*quinqies*, che estende il regime della responsabilità amministrativa dell'ente anche in relazione alla commissione dei delitti contro la personalità individuale disciplinati dalla Sezione I, Capo III, Titolo XII, Libro II c.p.; l'art. 25-*sexies*, ad opera dell'art. 9, comma 3, legge 18 aprile 2005, n. 62 ("legge

²⁰ Si tratta dei reati di falsità in bilancio, nelle relazioni e nelle altre comunicazioni sociali, falso in prospetto, falsità nelle relazioni o comunicazioni della società di revisione, impedito controllo, formazione fittizia del capitale, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, indebita ripartizione dei beni sociali da parte dei liquidatori, indebita influenza sull'assemblea, agguattaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza. Si ricorda che tale novero di reati è stato di recente ulteriormente ampliato ad opera dell'art. 31, comma 2, legge 28 dicembre 2005, n. 262 (recante "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari"), il quale ha inserito nell'art. 25-*ter* d.lgs. 231/2001 il delitto di omessa comunicazione del conflitto di interessi previsto dall'art. 2629-*bis* c.c., anche quest'ultimo articolo introdotto dallo stesso art. 31 legge 262/2005.

comunitaria 2004”), in relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla Parte V, Titolo I-bis, Capo II, d.lgs. 58/1998.

Nel corso del 2006 è stato poi inserito l’art. 25-*quater*.1 ad opera dell’art. 8, legge 9 gennaio 2006, n. 7, il quale ha esteso l’ambito di applicazione del d.lgs. 231/2001 al reato di pratiche di mutilazione degli organi genitali femminili, sono state apportate alcune modifiche all’art. 25-*quinquies* ad opera della legge 6 febbraio 2006, n. 38, “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo *internet*”. È stata prevista l’applicazione delle sanzioni indicate all’art. 10, in relazione alla responsabilità amministrativa degli enti per i reati previsti dall’art. 3 legge 16 marzo 2006, n. 146 (“Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall’assemblea generale il 15 novembre 2000 ed il 31 maggio 2001”) - per il quale si considera “reato transnazionale” il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Il 2007 ha poi visto l’introduzione dei reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro (art. 25-*septies*) ad opera della legge 3 agosto 2007, n. 123, art. 9, ed il reato di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-*octies*) ad opera del d.lgs. 21 novembre 2007, n. 231, art. 63, comma 3.

Le suddette Linee Guida di Confindustria, come quelle proposte dall’AIIA (Associazione Italiana *Internal Auditors*) e dall’ABI (Associazione Bancaria Italiana), rappresentano un “suggerimento” metodologico offerto - ai sensi dell’art. 6, comma 3, d.lgs. 231/2001 - dalle associazioni di categoria agli operatori che intendano avvalersi della facoltà loro riconosciuta dal medesimo art. 6, commi 1 e 2, i quali prevedono una possibile forma di “esonero” dalla responsabilità dell’ente se si dimostra, in occasione di un procedimento penale per uno dei reati considerati dalla norma: (i) di aver adottato ed efficacemente attuato, prima della commissione del fatto, Modelli di Organizzazione e di Gestione idonei a prevenire la realizzazione degli illeciti penali in questione; e (ii) di aver affidato il compito di vigilare sul funzionamento e l’osservanza dei suddetti Modelli, nonché di curarne l’aggiornamento, ad un organismo dell’ente che sia dotato di autonomi poteri di iniziativa e di controllo.

Poiché al fine di ottenere l’“esonero” dalle responsabilità dell’ente il giudice penale è chiamato a formulare, in occasione del procedimento penale a carico dell’autore materiale del fatto illecito, un giudizio di “idoneità” del sistema interno di organizzazione e controllo, che “deve spingersi sino alla capacità di prevenire rischi di reato prevedibili, alla luce delle conoscenze disponibili”²¹, risulta evidente che la formulazione dei Modelli e l’organizzazione dell’attività dell’organo di controllo debbano porsi come obiettivo l’esito positivo di tale giudizio di idoneità.

²¹ L’opportuna specificazione è di D. GALLETTI, *op. cit.*, p. 5.

Il d.lgs. 231/2001 tratteggia sinteticamente le caratteristiche che i Modelli di Organizzazione e di Controllo devono avere per poter affrontare l'esame di idoneità di cui all'art. 6, comma 3, prescrivendo che essi rispondano ad esigenze ben note a coloro che si occupano di implementare sistemi di *risk management*. Detti Modelli debbono, infatti, individuare le attività di "rischio", ossia quelle nel cui ambito possono essere commessi reati, prevedere specifici "protocolli" secondo i quali l'ente formerà ed attuerà le proprie decisioni, nonché modelli di gestione delle risorse finanziarie, al fine di prevenire il compimento di reati, introdurre obblighi informativi nei confronti dell'organismo deputato alla vigilanza, assieme ad un sistema disciplinare idoneo a sanzionare il mancato rispetto di quanto contenuto nel Modello di Organizzazione e di Gestione adottato.

A parte qualche indicazione che può trarsi dalla "Relazione di accompagnamento" poco è detto dal d.lgs. 231/2001 in merito all'Organismo di Vigilanza, mancanza che ha comportato non pochi problemi interpretativi in sede di prime applicazioni.

Limitandosi alla ricerca di punti di contatto tra la disciplina dettata dal d.lgs. 231/2001 e i *whistleblowing schemes*, si ricorda che l'Organismo di Vigilanza, il quale può essere composto da uno o più membri, dev'essere individuato all'interno della struttura societaria ("onde evitare facili manovre volte a preconstituire una patente di legittimità all'operato della *societas* attraverso il ricorso ad organismi compiacenti e soprattutto per fondare una vera e propria colpa dell'ente", recita la Relazione di accompagnamento) e deve rispondere ai requisiti di autonomia, indipendenza, professionalità e continuità d'azione che assicurino l'idoneità del medesimo a vigilare sul funzionamento e sull'osservanza dei Modelli adottati, nonché a verificarne costantemente l'aggiornamento e l'adeguamento, sia rispetto alle novità normative, sia con riferimento all'evoluzione della struttura aziendale²².

Ulteriore punto di contatto può essere desunto riportando l'attenzione sulla prescrizione contenuta nell'art. 6, comma 2, lett. *d*), d.lgs. 231/2001, il quale, come già anticipato, stabilisce che, tra le caratteristiche che i Modelli devono soddisfare, vi è la previsione di obblighi di informazione nei confronti dell'Organismo di Vigilanza. Il corretto adempimento di tale obbligo dovrebbe fornire un utile supporto all'attività di vigilanza dell'Organismo preposto, sia in una fase "fisiologica" (ossia preventiva rispetto al compimento di reati), consentendo una costante verifica circa il corretto funzionamento del Modello adottato, sia in un'eventuale fase "patologica" (una volta che il reato sia stato compiuto), quando spetta all'Organismo svolgere la relativa delicata attività di indagine ed accertamento circa l'accaduto.

Va da sé che l'obbligo informativo a favore dell'Organismo di Vigilanza, dovrebbe gravare non solo sui soggetti posti in posizione "apicale", in relazione ai cui ambiti di attività sono state verosimilmente accertate le "zone di rischio" da sorvegliare, ma anche sui dipendenti che in qualsiasi modo e momento possano venire a conoscenza di attività o comportamenti in contrasto con quanto prescritto in forza dei Modelli di Organizzazione e Gestione adottati ai sensi del d.lgs. 231/2001. Di qui, l'esigenza che detti Modelli prevedano, al proprio interno ovvero in separati testi, un'apposita regolamentazione delle modalità secondo le quali realizzare un efficace sistema di

²² Per una puntuale analisi critica relativa alla corretta individuazione dell'Organismo di Vigilanza ai sensi del d.lgs. 231/2001, si veda, ancora, D. GALLETTI, *op. cit.*, pp. 6 ss..

reporting di fatti e/o comportamenti concreti che consenta al personale di riferire casi di violazione di norme da parte di altri soggetti all'interno della società, ossia, prendendo in prestito il suggestivo termine anglosassone, di *whistleblowing schemes*.

4.2 L'adozione e l'implementazione dei *whistleblowing schemes* in ambito societario italiano. Valutazione delle criticità connesse

Il rapido *detour* appena compiuto in tema di responsabilità amministrativa delle persone giuridiche, consente di ben cogliere come l'adozione, l'implementazione e la gestione di sistemi di *reporting* necessiti, in primo luogo, di una compiuta definizione di figure, norme e procedure atte a disciplinare gli aspetti organizzativi dell'intero processo in cui si dipanano detti sistemi. Particolare attenzione andrà posta, da un lato, all'individuazione dei ruoli, dei compiti, delle funzioni e delle connesse responsabilità per la gestione delle varie fasi del trattamento dei dati e delle informazioni raccolti, nonché, dall'altro, all'adozione di univoche e puntuali procedure nel cui rispetto detti dati ed informazioni dovranno essere utilizzati.

Può a questo punto essere utile tentare di ipotizzare i passaggi necessari (o anche solo opportuni) per l'adozione e l'implementazione di *whistleblowing schemes* nell'ambito di una realtà societaria italiana, anche sulla scorta dei principi guida offerti dal Parere WP117.

(i) *Delibera dell'organo societario competente. Possibile ruolo degli amministratori "indipendenti" e del "comitato per il controllo interno"*

L'adozione di un *whistleblowing scheme* dovrà in primo luogo essere oggetto di un'apposita delibera assunta dall'organo amministrativo della società, nell'ambito della quale dovranno essere opportunamente chiarite le finalità sottese a tale adozione, nonché, assieme ai benefici, le problematiche ad essa connesse.

In particolare, sarà opportuno che l'organo deliberante prenda atto della circostanza che l'adozione di adeguati schemi di flussi informativi interni è finalizzata a consentire, come già scritto, una corretta applicazione dei principi di *corporate governance* nell'ambito della quotidiana attività societaria, fornendo un efficace supporto alle funzioni interne aziendali deputate alle attività di *reporting*, del quale beneficerebbero, in ultima istanza, i vertici aziendali. Peraltro, il corretto funzionamento di tali procedure potrà costituire un prezioso ausilio per quello specifico compito istituzionalmente attribuito all'organo amministrativo consistente nella valutazione circa l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società, previsto dall'art. 2381, comma 3, c.c..

Allo stesso tempo, l'organo amministrativo dovrebbe prendere coscienza del fatto che l'adozione di tale tipo di procedure comporta un'inevitabile trattamento di ingenti quantità di dati personali, con le connesse questioni attinenti, tra l'altro, la disciplina posta a tutela della riservatezza dell'individuo segnalante e di quello segnalato.

La chiara indicazione delle finalità sottese all'adozione di simili procedure appare ancor più opportuna alla luce della circostanza che "fonte legittimante" delle stesse non è rinvenibile - ad oggi - in obblighi normativi diretti, ma trova invece la sua

giustificazione (e quindi, si sarebbe tentati di scrivere, legittimazione) nella considerazione che l'adozione di idonee regole di *corporate governance* appaiono idonee ad assicurare un elevato livello di trasparenza e correttezza nelle pratiche attinenti il settore finanziario e amministrativo in generale delle società, con benefiche ricadute sulla protezione degli *stakeholders* e sulla solidità dell'intero sistema economico.

Con la medesima delibera, l'organo amministrativo potrà individuare al proprio interno e/o tra le altre possibili funzioni aziendali ritenute più idonee a questo fine alcune figure, in numero adeguato alla dimensione societaria e con l'eventuale supporto di professionisti esterni, alle quali delegare il compito di elaborare in concreto una procedura (laddove non già sviluppata in seno al medesimo organo amministrativo) atta a soddisfare le finalità descritte nella stessa delibera, opportunamente "contestualizzata" nella specifica realtà aziendale nota ai soggetti delegati. A queste stesse figure l'organo amministrativo potrà fare riferimento anche per quanto riguarda la funzione di supervisione in merito al generale funzionamento del *whistleblowing scheme*, sempre nel rispetto dell'autonomia e dell'indipendenza dei soggetti ad esso preposti.

Sulla scorta della già menzionata Raccomandazione della Commissione 2005/162/CE e di quanto più esplicitamente indicato nel "Codice di autodisciplina" elaborato dal Comitato per la *Corporate Governance* di Borsa Italiana SpA (edizione marzo 2006), per entrambe gli scopi di cui sopra (elaborazione del *whistleblowing scheme* e supervisione in merito al suo funzionamento), l'organo amministrativo (in particolare quello delle società di maggiori dimensioni) potrà, con l'obiettivo di incrementare l'efficienza e l'efficacia dei propri lavori, costituire specifici comitati aventi funzioni consultive e propositive, i quali "lungi dal sostituirsi al consiglio nell'adempimento dei propri doveri, possono utilmente svolgere un ruolo istruttorio - che si esplica nella formulazione di proposte, raccomandazioni e pareri - al fine di consentire al consiglio stesso di adottare le proprie decisioni con maggiore cognizione di causa".

Ai fini di cui sopra, un ruolo fondamentale potrebbe essere attribuito al "comitato per il controllo interno" e, in un'ottica "atomistica", agli amministratori "indipendenti" dei quali il menzionato comitato dev'essere per la maggior parte, se non esclusivamente, composto.

Quanto al "comitato per il controllo interno", ad esso (o meglio all'*audit committee*) e alla sua possibile funzione relativa ai *whistleblowing schemes* fa espressamente riferimento la stessa Raccomandazione della Commissione 2005/162/CE, secondo la quale "il comitato per la revisione dei conti" (questa la traduzione di *audit committee* nel testo italiano della Raccomandazione) "dovrebbe esaminare la procedura in base alla quale la società rispetta le disposizioni in vigore relative alla possibilità per i dipendenti di segnalare presunte irregolarità gravi che si verificano nella società, presentando una denuncia o attraverso segnalazioni anonime a un amministratore indipendente. Esso dovrebbe inoltre assicurarsi che esistano strumenti per lo svolgimento di indagini indipendenti e proporzionate su tali questioni e che sia previsto un seguito adeguato" (punto 4.3.8 dell'Allegato I alla Raccomandazione).

Tra le funzioni che la Raccomandazione attribuisce al "comitato per il controllo interno" vi è infatti quella di assistere il consiglio d'amministrazione nel riesaminare periodicamente i sistemi di controllo interno e di gestione dei rischi, al fine di

garantire che i rischi principali, ivi compresi quelli connessi al rispetto della legislazione e dei regolamenti aziendali esistenti, siano correttamente individuati, gestiti e resi noti ai rispettivi destinatari.

Anche la figura dell'amministratore "indipendente", così come le caratteristiche che lo stesso deve avere, sono ora positivamente normate; ad esso fa infatti ora cenno l'art. 2387 c.c. e, più estesamente, l'art. 147-ter, comma 4, d.lgs. 24 febbraio 1998, n. 58, a seguito delle modifiche apportate dalla legge 28 dicembre 2005, n. 262, e, successivamente, dal d.lgs. 29 dicembre 2006, n. 303, e, ancor più, l'art. 3 del suddetto "Codice di autodisciplina" di Borsa Italiana SpA.

Senza pretesa di esaustività²³, ma ai soli e limitati fini di tentare di valutare la correttezza dello specifico ruolo che qui s'intende attribuire a tale figura, si ricorda che l'amministratore si qualifica come "indipendente" quando non è esecutivo, ossia non è direttamente coinvolto nella gestione della società e non ha in essere, né ha di recente intrattenuto con la società (e, in particolare, il suo *management*) e con l'azionariato di riferimento o in grado di influenzare la gestione della società, relazioni tali da condizionarne l'autonomia di giudizio. La valutazione in merito all'"indipendenza", è rimessa al consiglio d'amministrazione e dev'essere svolta all'atto della nomina e, successivamente, con cadenza almeno annuale, essendo essa qualificabile come un requisito dinamico.

Gli "amministratori indipendenti" devono pertanto essere in grado di fornire un giudizio *super partes*, autonomo e non condizionato per tutta la durata del loro incarico. La presenza di tali figure, chiamate a svolgere una costante attività di monitoraggio sulle deliberazioni consiliari e, in generale, sul *management* della società, dovrebbe facilitare ed essere di supporto ad una corretta ed imparziale gestione dell'impresa. D'altronde, è opinione condivisa che l'amministratore consapevole dei propri doveri, connessi alle funzioni che gli sono attribuite, agisca sempre con indipendenza di giudizio, come ben evidenziato nel "Codice di autodisciplina", il quale ricorda come l'indipendenza di giudizio debba essere requisito delle decisioni di tutti gli amministratori, siano essi esecutivi o non esecutivi, e siano o meno "indipendenti".

In ragione di quanto sopra accennato, si ritiene che tanto il "comitato per il controllo interno", quanto l'amministratore "indipendente", per le posizioni apicali che ricoprono e le accennate qualità che devono soddisfare, siano figure idonee per la funzione di supervisione del *whistleblowing scheme* che fosse eventualmente attuato²⁴. Pur non essendo la figura dell'"amministratore indipendente" usualmente

²³ Per un'autorevole introduzione giuridica alla figura dell'amministratore indipendente si rimanda, fra tutti, a F. BONELLI, *Gli amministratori di SpA dopo la riforma delle società*, Giuffrè, 2004, pp. 108 ss.. Offre un efficace ed ampio panorama sul mondo degli amministratori indipendenti il sito *web* www.nedcommunity.it. A testimonianza del sempre maggiore interesse che suscita il ruolo dell'amministratore indipendente anche tra le categorie professionali alle quali tale ruolo potrebbe essere rivolto, si menziona l'iniziativa assunta nel corso del 2008 dall'Ordine degli Avvocati di Milano e dalla Fondazione Forense di Milano che, nell'ambito dell'attività di formazione professionale continua, ha organizzato un intero corso avente ad oggetto l'analisi della figura dell'amministratore indipendente (www.ordineavvocatimilano.it).

²⁴ Si esprime in tal senso anche il già citato PCAW nel proprio *Policy Paper-Governance* del 2002 dal titolo *NEDs and whistleblowing* sul ruolo che i NEDs (*Non Executive Directors*) dovrebbero avere nell'ambito dei *whistleblowing schemes* (il documento è consultabile all'indirizzo *internet*: http://www.pcaw.co.uk/policy_pub/non_executive_directors_review.html). In particolare, il PCAW si esprime così: "As importantly, such a NED role is likely to encourage the Board to view its whistleblowing policy more as a cultural issue than as one of tick-box compliance. This will help the Board not only to assert its accountability down through the company but also to demonstrate it - and also the role and efficacy of its NEDs - to shareholders and other stakeholders".

nota alle medie e grandi imprese non quotate italiane, si ritiene tuttavia che essa possa svolgere, proprio per la sua funzione *super partes*, un ruolo decisivo per una corretta gestione anche in realtà imprenditoriali di modeste dimensioni.

(ii) Peculiarità nel contesto dei gruppi di società

Una situazione maggiormente complessa potrebbe aversi per società facenti parte di gruppi nell'ambito dei quali l'elaborazione degli schemi organizzativi in commento sia rimessa alle società capogruppo, analogamente a quanto si assiste in relazione ai codici di condotta in materia di 231/2001, ovvero in relazione ai mansionari *privacy* e ai "Documenti Programmatici sulla Sicurezza" ai sensi del d.lgs. 196/2003, ovvero ancora, per certi versi, a proposito delle relazioni in punto di valutazione dei rischi per la sicurezza e la salute sui luoghi di lavoro ai sensi del d.lgs. 626/1994, nonché, infine, delle certificazioni di qualità. Il grado di complessità aumenterebbe nel caso di gruppi societari nei quali la capogruppo risultasse essere di nazionalità diversa da quella italiana.

In entrambe i casi, l'organo amministrativo chiamato ad adottare nella società dal medesimo gestita le procedure, gli schemi, i protocolli e/o i codici di condotta elaborati da terzi soggetti - per quanto infragruppo - sarebbe in ogni caso tenuto ad una valutazione che, se nel caso di capogruppo di nazionalità italiana potrebbe limitarsi ad un'analisi di compatibilità alle caratteristiche proprie della specifica realtà aziendale, nel caso di casa madre di nazionalità estera dovrebbe altresì spingersi ad una verifica di liceità, rispetto alle prescrizioni normative applicabili, delle concrete modalità di funzionamento di detti schemi.

L'onere (o piuttosto il dovere) di procedere a dette valutazioni conseguirebbe per la società di destinazione del *whistleblowing scheme*, oltreché dal rapporto contrattuale in essere tra la stessa società ed i propri dipendenti ai quali tale schema sarebbe rivolto, anche dalla circostanza che difficilmente la società potrebbe sottrarsi alla qualifica di "titolare" ovvero di "responsabile" del trattamento dei dati personali, con i conseguenti obblighi di legge che incombono su tali soggetti in materia di protezione dei dati personali²⁵.

(iii) Cenni in punto di possibili ulteriori verifiche di legittimità

Nell'ambito dell'ordinamento italiano, l'attuazione dei *whistleblowing schemes* potrebbe doversi confrontare, oltreché con la normativa dettata a protezione dei dati

²⁵ Chiara appare la presa di posizione sul punto della già menzionata autorità francese CNIL, secondo la quale "Il est vrai que la mise en place d'un dispositif d'alerte peut avoir été imposée par la maison-mère du groupe, établie à l'étranger, et que la société française n'a qu'une marge de manoeuvre restreinte dans sa mise en oeuvre. Il peut même être prévu que les alertes soient ainsi collectées directement auprès de la maison-mère, ou par le prestataire désigné par celle-ci. Une organisation de la collecte à l'étranger ne conduit pas à exclure l'application de la loi du 6 janvier 1978. En effet, la société française est seule compétente pour respecter les procédures de consultation des instances représentatives du personnel et d'information individuelle des salariés, organiser le traitement des données lors de la vérification des faits réalisée en son sein, ordonner et faire appliquer les mesures correctives nécessaires pour remédier à des dysfonctionnements, et éventuellement sanctionner leurs auteurs. L'autonomie de la société française dans l'organisation du traitement des alertes, même si elle n'est parfois que relative à certains stades de ce processus, reste suffisante pour justifier sa qualification de responsable de traitement" (FAQ sur les dispositifs d'alerte professionnelle, n. 9).

personali, anche, ad esempio, con la disciplina in materia di controlli sul personale dipendente.

I moderni mezzi tecnologici di cui un *whistleblowing scheme* potrebbe avvalersi²⁶ pongono infatti in primo piano anche la questione relativa al “controllo a distanza” del lavoratore. La tutela della dignità e riservatezza del lavoratore sul luogo di lavoro, di fronte alle esigenze di controllo a distanza del datore di lavoro, dovrebbe costituire quindi ulteriore argomento di riflessione nella verifica di legittimità in parola, alla luce dell’art. 4 legge 20 maggio 1970, n. 300 (cd. “Statuto dei lavoratori”)²⁷.

Detta attività di verifica potrà spingersi sino a valutare la liceità dell’attività di controllo, ad esempio, della corrispondenza altrui, ove a ciò porti l’implementazione dello schema in commento. Tale riflessione risulta ancora più necessaria ove si consideri che l’art. 15 della Costituzione italiana, posto a caposaldo del principio di inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, è stato ulteriormente ribadito e rafforzato dalla legge 23 dicembre 1993, n. 547, in tema di criminalità e reati informatici²⁸, e dal d.lgs. 7 marzo 2005, n. 82 (“Codice dell’amministrazione digitale”), sul documento elettronico²⁹.

Una qualsiasi analisi del problema ad opera dell’organo amministrativo, così come ipotesi di soluzione del medesimo, non potrebbe dunque prescindere dai principi inderogabili posti dalle suddette prescrizioni normative in materia di protezione dei dati personali, di fedeltà del dipendente e di controllo di quest’ultimo.

(iv) Elementi essenziali di un whistleblowing scheme

Conclusa la fase deliberativa (ma non anche quella di supervisione ad opera dell’organo amministrativo, di carattere necessariamente continuativo, come si è già accennato sopra), il *whistleblowing scheme* dovrà essere concretamente elaborato e, quindi, successivamente attuato, avendo specificamente individuato i soggetti, i mezzi, i luoghi e le procedure attraverso i quali lo schema sia in grado di funzionare e, comunque, nel rispetto dei già menzionati principi di qualità e proporzionalità dei

²⁶ È interessante notare come con sentenza del 16 giugno 2000, n. 8250, la Corte di Cassazione, Sezione Lavoro, abbia espressamente statuito che la fattispecie vietata dall’art. 4 legge 300/1970, sia per la formulazione in un certo senso generica degli strumenti di controllo, sia per l’ampiezza dell’oggetto tutelato, che include i diritti di libertà, dignità e di riservatezza del lavoratore, viene a dipendere e ad inserirsi in un contesto informatico, tecnologico e del sistema di comunicazioni in continua evoluzione e, come tale, essa consente la tutela del lavoratore di nuovi e più sofisticati mezzi di controllo.

²⁷ Nel rispetto dei limiti del presente contributo, si ricorda soltanto che l’art. 4 legge 300/1970 vieta, com’è noto, in generale, l’utilizzo di impianti o apparecchi che hanno la finalità esclusiva di controllare a distanza l’attività dei lavoratori. Al di fuori di tale caso, l’art. 4 prevede la possibilità di utilizzare gli impianti di controllo a distanza, se ciò è motivato da esigenze organizzative, produttive o di sicurezza del lavoro. In presenza di tali presupposti il datore di lavoro, per poter installare gli impianti di controllo, deve tuttavia raggiungere un accordo con le rappresentanze sindacali, oppure, in mancanza di tale accordo, chiedere l’autorizzazione alla Direzione provinciale del lavoro, settore ispettivo. Quest’ultima può dare parere favorevole, oppure accordare l’autorizzazione dettando nel contempo le modalità con cui effettuare l’uso di detti impianti o, infine, respingere la domanda, salva la possibilità del datore di lavoro di presentare ricorso entro 30 giorni al Ministero del Lavoro.

²⁸ Il riferimento è in particolare all’art. 616, comma 4, c.p., il quale nel punire la violazione, sottrazione e soppressione di corrispondenza, afferma che per “corrispondenza” s’intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

²⁹ Il riferimento in questo caso è all’art. 49 del citato d.lgs. 82/2005, il quale sancisce la segretezza della corrispondenza trasmessa per via telematica.

dati trattati, “trasparenza” nell’adozione e nell’applicazione delle procedure, rispetto dei diritti dei soggetti segnalati, sicurezza dei sistemi di trattamento dei dati e corretta gestione delle procedure³⁰.

(iv).a Soggetti preposti

Quanto ai soggetti, specie nelle società di grandi dimensioni, dovranno essere appositamente nominate figure operative dedicate all’attività di raccolta e (quantomeno di prima) gestione delle segnalazioni.

Detti soggetti preposti dovranno essere dotati di una struttura adeguata per organizzazione e mezzi, specificamente istruiti a svolgere tale funzione, nonché vincolati a severi obblighi di riservatezza e confidenzialità. Essi dovranno operare secondo procedure e schemi di *reporting* che, per quanto possibile, siano standardizzati ed univoci, non solo al fine di facilitarne la successiva gestione, ma anche nell’intento di limitare al massimo la possibile influenza di giudizi ed opinioni personali, che necessariamente differirebbero tra i diversi soggetti preposti di volta in volta coinvolti.

Alla stregua di quanto suggerito dal Gruppo di lavoro, tali strutture dovranno essere autonome ed indipendenti rispetto al resto dell’organizzazione societaria, con obbligo di riferire soltanto e direttamente ai soggetti interni alla società dotati del potere di assumere le decisioni del caso, anch’essi vincolati ad impegni di riservatezza e confidenzialità. Tutte caratteristiche, queste accennate, che ricordano da vicino quelle che il “Codice di autodisciplina” di Borsa Italiana SpA ha inteso attribuire ai “soggetti preposti al controllo interno”, il cui ruolo consiste essenzialmente nel verificare che il sistema di controllo interno sia sempre adeguato, pienamente operativo e funzionante (criterio 8.C.6. del Codice).

Nulla vieta che tali soggetti siano individuati all’esterno della società, in organizzazioni - note per ora quasi esclusivamente alla prassi statunitense³¹ - specializzate nella gestione delle cd. *hotlines*. Il vantaggio sarebbe rappresentato da una verosimile maggiore “indipendenza” e “neutralità” d’azione rispetto al personale dipendente, costretto, quest’ultimo, tra una più “ingombrante” attiguità con i superiori gerarchici, per un verso, ed un’“emarginante” diffidenza dei colleghi, per altro verso. Tali strutture, non solo in quanto (almeno sulla carta) maggiormente professionali, ma anche per il sol fatto di essere fisicamente dislocate in luoghi distinti da quelli di lavoro, potrebbero altresì assicurare un più elevato di riservatezza.

Tali soggetti dovrebbero essere qualificati, ai sensi della disciplina posta a tutela del trattamento di dati personali, quali “responsabili” del trattamento (secondo la definizione degli artt. 4, comma 1, lett. g), e 29 d.lgs. 196/2003) di dati dagli stessi raccolti; qualifica, questa che mentre non pone particolari problemi ove i soggetti preposti siano dipendenti della società, potrebbe porne nel caso di soggetti ad essa esterni, dovendo il “titolare” del trattamento, ossia la società nella quale il

³⁰ Per un’approfondita descrizione degli elementi costitutivi e procedurali dei *whistleblowing schemes*, si veda C. FLORIO, *op. cit.*, p. 929.

³¹ Una delle più note società statunitensi, attive in tale settore sin dall’inizio degli anni ’80 con la denominazione di *AlertLine*, è la *Global Compliance* (www.globalcompliance.com). In ambito comunitario il riferimento più noto è alla già menzionata organizzazione *Public Concern at Work* (“PCaW”) (www.pcaw.co.uk), attiva dal 1993.

whistleblowing scheme è implementato (secondo la definizione degli artt. 4, comma 1, lett. *f*), e 28 d.lgs. 196/2003) conferire formali istruzioni per la corretta esecuzione dei compiti affidati e porre altresì in essere una costante attività di vigilanza sui medesimi al fine di verificare il rispetto degli obblighi di legge e negoziali.

Tra i compiti demandati ai soggetti preposti rientrerebbero certamente quelli di consentire ai soggetti “interessati” (secondo la definizione dell’art. 4, comma 1, lett. *i*), d.lgs. 196/2003) l’esercizio dei diritti di cui agli artt. 7 ss. d.lgs. 196/2003, ricorrendone i presupposti di applicabilità³².

(iv).b Sicurezza dei dati e delle informazioni

Come già scritto, i soggetti che adottino i *whistleblowing schemes* dovranno attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali così raccolti dalla distruzione accidentale o illecita, dalla perdita accidentale o dall’alterazione, dalla diffusione o dall’accesso non autorizzati, nonché imporne il rispetto da parte dei soggetti preposti.

A tale proposito, sarà imprescindibile fare riferimento all’art. 31 d.lgs. 196/2003, il quale prescrive che i dati personali oggetto di trattamento siano custoditi e controllati - anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento - in modo da ridurre al minimo, mediante l’adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A tali “idonee” misure di sicurezza dovrà fare riferimento il titolare che intenda provare di essere esente dalla responsabilità civile ai sensi dell’art. 2050 c.c., stabilita dall’art. 15 d.lgs. 196/2003.

Le concrete misure “minime” di sicurezza da adottare sono indicate negli artt. 33, 34 e 35 d.lgs. 196/2003, come meglio specificate nell’allegato B), alle quali disposizioni - per esigenze di spazio - si fa integrale rimando. In questa sede si rammenta solo quanto stabilito dall’art. 33, secondo il quale i titolari dei trattamenti sono in ogni caso tenuti ad adottare le misure “minime” individuate negli stessi artt. 33, 34 e 35 ovvero ai sensi dell’art. 58, comma 3 (il quale prevede il periodico aggiornamento delle misure di sicurezza con decreto del Presidente del Consiglio dei Ministri), pena l’imputabilità di carattere penale prevista dall’art. 169 d.lgs. 196/2003.

In tema di misure di sicurezza, si precisa che esse non sono soltanto “fisiche”, aventi ad oggetto la protezione di luoghi ed apparecchiature, e “logiche”, ossia riguardanti la protezione delle informazioni gestite con i sistemi informativi, ma anche e in primo luogo “organizzative”, il che pone nuovamente l’accento sulla centralità delle norme e delle procedure idonee a disciplinare l’aspetto organizzativo sottostante all’implementazione degli schemi in esame.

³² I diritti riconosciuti dall’art. 7 sono essenzialmente quelli dell’accesso, della modifica e dell’opposizione al trattamento dei dati personali. Evidentemente, nell’ambito di un trattamento di dati personali posto in essere in ragione di una segnalazione operata in un *whistleblowing scheme*, tali diritti potranno subire una “compressione” ai sensi e per gli effetti dell’art. 8, comma 2, lett. *e*), d.lgs. 196/2003, limitatamente al periodo durante il quale il loro esercizio potrebbe causare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l’esercizio di un diritto in sede giudiziaria.

L'aspetto della sicurezza (ivi compresa la formazione) sarà di maggiore momento per la società presso la quale il *whistleblowing scheme* dev'essere implementato, nel caso in cui la scelta in merito all'individuazione dei soggetti preposti ricada su personale dipendente operante all'interno della medesima società. In tal caso, infatti, tale personale dovrà essere dotato di mezzi di comunicazione ed elaborazione (telefono fisso e mobile, *fax*, computer fisso e mobile, stampanti, programmi informatici, archivi fisici, ecc.) ed essere ubicato in locali adeguatamente dedicati allo svolgimento di tale delicata attività.

La questione sicurezza avrà ad oggetto non soltanto le iniziali fasi della raccolta e della prima gestione dei dati personali contenuti nelle segnalazioni, ma anche le fasi della conservazione ovvero della distruzione degli stessi.

A fronte di ciascuna segnalazione, i soggetti preposti dovranno infatti compiere un'attenta e delicata valutazione alla quale dovrebbe conseguire l'immediata distruzione dei rapporti dagli stessi predisposti sulla base delle informazioni ricevute, ove le stesse apparissero palesemente ed integralmente estranee alle finalità del *whistleblowing scheme* adottato, ovvero raccolte, trattate e conservate, nel caso di loro conformità e rilevanza. Si tratterebbe, tuttavia, di un primo periodo di conservazione, che, stando a quanto affermato nel "WP117", non potrebbe superare i 2 mesi dalla conclusione delle indagini "interne" alla società.

Decorso tale primo periodo, le segnalazioni (*rectius*, i dati personali in esse contenuti) potranno essere ulteriormente conservati solo in caso di inizio di un'azione disciplinare o giudiziaria da parte della società, diversamente dovendosi procedere ad una loro distruzione o, quantomeno, se ritenuto di interesse per la società, ad un procedimento di "anonimizzazione" dei dati personali presenti nelle segnalazioni³³.

(iv).c Informativa agli interessati - Consenso degli interessati - Autorizzazione del Garante per la protezione dei dati personali - Notificazione al Garante per la protezione dei dati personali

- Informativa agli interessati

Passando all'analisi degli aspetti più squisitamente procedurali, si evidenzia che l'implementazione dei *whistleblowing schemes* dev'essere accompagnata da un'adeguata, completa e chiara informativa a favore dei soggetti potenzialmente qualificabili come "interessati".

Tale *disclosure* deve avere ad oggetto non solo l'esistenza, le finalità e il funzionamento (compresa l'individuazione dell'organismo incaricato della

³³ Parzialmente diversa risulta la posizione espressa dall'autorità francese CNIL, secondo la quale "Si l'alerte ne rentre pas dans le champ du dispositif, la destruction ou l'archivage des données s'y rapportant doivent être réalisés sans délai. Si l'alerte rentre dans le champ du dispositif, l'organisation chargée de la gestion des alertes procède à la vérification des faits recueillis et dispose de deux mois, à compter de la fin de ces opérations de vérification, pour communiquer ses conclusions ainsi que les informations nécessaires aux personnes compétentes définies par l'employeur. A l'issue de cette période de deux mois (i) soit l'employeur décide d'engager une procédure disciplinaire ou judiciaire, les données détenues par l'organisation chargée de la gestion des alertes peuvent être conservées jusqu'au terme de la procédure; (ii) soit l'employeur décide de ne pas donner suite à l'alerte, les données s'y rapportant sont détruites ou archivées sans délai. Le choix entre la destruction ou l'archivage des données relatives aux alertes appartient à l'employeur. L'archivage s'entend par la conservation des données dans un système d'information distinct à accès restreint. En cas d'archivage, les données peuvent être conservées pendant une durée maximale de trente ans" (FAQ sur les dispositifs d'alerte professionnelle, n. 17).

raccolta) delle segnalazioni, ma deve rappresentare altresì il diritto di accesso, rettifica e cancellazione dei dati raccolti da parte dei soggetti "interessati" (artt. 7 ss. d.lgs. 196/2003).

In un contesto societario, sarebbe quindi opportuno procedere alla divulgazione delle suddette informazioni presso il personale dipendente, con l'ausilio dell'ufficio del personale, prima di attivare lo stesso schema.

L'informativa, soggetta ad aggiornamento in caso di variazione di uno o più degli elementi in essa contenuti ai sensi dell'art. 13 d.lgs. 196/2003, potrebbe essere messa a disposizione dei dipendenti mediante affissione nelle bacheche, ovvero, se disponibile, con il più moderno sistema di *intranet* aziendale. Potrebbe altresì essere opportuno rendere conoscibile al soggetto che intenda effettuare una segnalazione il contenuto dell'informativa mediante comparsa del relativo testo a video al momento dell'accesso al sistema di comunicazione elettronica (nel caso si sia optato per un *web reporting vehicle*), ove il destinatario risulti essere il soggetto preposto alla ricezione di tale tipo di comunicazioni. Ovvero, in caso di *whistleblowing schemes* che si avvalgano del mezzo telefonico (le già menzionate *hotlines*), potrebbe essere opportuno predisporre un sistema di *voice messaging* con il testo dell'informativa (o una sua sintesi) attivato all'inoltro di ogni telefonata.

- Consenso degli interessati

Non sarà invece necessario (e, invero, neppure opportuno) richiedere da subito ai dipendenti della società (nella duplice possibile veste di soggetti segnalanti e di soggetti segnalati) un espresso consenso per il trattamento dei relativi dati personali, in quanto il trattamento sarebbe in tale fase solo potenziale e non effettivo (potendo, in teoria, non verificarsi mai alcuna segnalazione) e riguarderebbe dati personali solo astrattamente e del tutto genericamente ipotizzabili *a priori* (ad esempio, comportamenti apparentemente contrari a norme di legge o di regolamenti aziendali).

A fronte di ogni segnalazione, sarà invece imprescindibile verificare la necessità di richiedere il consenso del dipendente autore della stessa, nonché (più problematicamente) di colui che ne fosse oggetto, assumendo entrambe in tal caso, nei confronti della società, la veste di soggetti "interessati" ai sensi del d.lgs. 196/2003.

Quanto al primo, la volontarietà della segnalazione e la non anonimità della stessa (ove la scelta fosse in tal senso, come si dirà più avanti), dovrebbe far ritenere l'ottenimento del consenso non irto di particolari difficoltà.

Del tutto diversa appare la situazione del soggetto "interessato" segnalato. Sarà in proposito necessario verificare di volta in volta la natura dei dati personali contenuti nella segnalazione, ossia se qualificabili come "comuni" (art. 1, comma 1, lett. *b*), d.lgs. 196/2003), "sensibili" (art. 1, comma 1, lett. *d*), d.lgs. 196/2003), "giudiziari" (art. 1, comma 1, lett. *e*), d.lgs. 196/2003) o, come da alcuni definiti, "super sensibili" (art. 17, comma 1, d.lgs. 196/2003), avendo ciascuno di essi un diverso livello di tutela (e di connessa disciplina), in ragione della maggiore potenziale lesività che potrebbe conseguire da un illecito trattamento dei medesimi.

Tra le ipotesi di esenzione dalla richiesta del consenso, pare più verosimilmente ricorribile nell'ambito del funzionamento di un *whistleblowing scheme* quella

connessa al trattamento necessario per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (art. 24, comma 1, lett. *f*). In caso di dati personali “sensibili” idonei a rivelare lo stato di salute e la vita sessuale, il diritto dev’essere di rango pari a quello dell’interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 26, comma 4, lett. *c*). Quanto ai dati “giudiziari”, il loro trattamento è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante per la protezione dei dati personali, che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 27 d.lgs. 196/2003). Infine, con una sorta di norma di chiusura, l’art. 17 prescrive che il trattamento dei dati diversi da quelli “sensibili” e “giudiziari” che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell’interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell’interessato, ove prescritti dal Garante, nell’ambito di una verifica preliminare all’inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

- Autorizzazione del Garante per la protezione dei dati personali

Il quadro disciplinare si complica ulteriormente ricordando che il trattamento dei dati “sensibili” (art. 26 d.lgs. 196/2003) è consentito, oltreché con il consenso dell’interessato (necessario salvo quanto scritto sopra), previa autorizzazione del Garante, il quale, come già accennato, è chiamato ad intervenire anche in relazione ai dati “giudiziari” (art. 27 d.lgs. 196/2003) e ai dati “super sensibili” (art. 17 d.lgs. 196/2003).

Mentre per i primi e per i secondi il riferimento di disciplina è all’Autorizzazione n. 1/2007 (“Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro”)³⁴ e all’Autorizzazione n. 7/2007 (“Autorizzazione al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici”)³⁵, entrambe efficaci sino al 30 giugno 2008, nessun provvedimento recante “le misure e gli accorgimenti” di cui al citato art. 17 risulta essere stato sinora emanato con riferimento ai dati “super sensibili”.

³⁴ Nell’ambito del funzionamento di un *whistleblowing scheme* l’unico riferimento autorizzativo possibile pare essere all’art. 3, lett. *d*, autorizzazione n. 1/2007, secondo il quale il trattamento dei dati “sensibili” dev’essere “indispensabile per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere dev’essere di rango pari a quello dell’interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile”.

³⁵ In maniera molto più netta e limitativa, il Garante ha ritenuto che il trattamento dei dati “giudiziari” dev’essere “indispensabile per adempiere o per esigere l’adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario” (art. 1, Capo I, autorizzazione n. 7/2007).

Considerando i ristrettissimi margini di manovra consentiti alla società che, avendo implementato un *whistleblowing scheme*, si trovi a dover trattare, in veste di “titolare”, dati personali “sensibili”, “giudiziari” e “super sensibili”, massimamente utile sarebbe un riscontro del Garante sollecitato ad esprimere un parere ai sensi dell’art. 154 d.lgs. 196/2003³⁶.

- Notificazione al Garante per la protezione dei dati personali

Il d.lgs. 196/2003 pone la necessità di verificare l’applicabilità, nell’attuazione e nel funzionamento di un *whistleblowing scheme*, dell’ulteriore obbligo rappresentato dalla notificazione al Garante per la protezione dei dati personali, ai sensi dell’art. 37.

L’adempimento rappresentato dalla notificazione al Garante è forse quello che ha subito con il d.lgs. 196/2003 il mutamento di disciplina più drastico. Si ricorda, infatti, che l’art. 7 legge 675/1996 (o meglio una sua modifica apportata con d.lgs. 28 luglio 1997, n. 255), stabiliva che il titolare che intendesse procedere ad un trattamento di dati personali era tenuto a darne notificazione al Garante, salvo il ricorrere di una serie di esenzioni di carattere parziale ovvero totale. Oggi, l’art. 37 d.lgs. 196/2003 dispone invece che il titolare notifichi al Garante il trattamento di dati personali al quale intende procedere, solo se il trattamento riguardi una serie di ipotesi specificamente individuate.

Tra le ipotesi di obbligo di notificazione, vi è quella che dispone che il titolare notifichi al Garante il trattamento di dati personali cui intende procedere, se il trattamento riguarda, tra gli altri, dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni e - per quanto più direttamente ci interessa - a comportamenti illeciti o fraudolenti (art. 37, comma 1, lett. *f*)).

Per quanto la suddetta disposizione sia stata dettata avendo a mente le cd. “centrali rischi” pubbliche e private³⁷, gli elementi descrittivi dei quali essa si compone paiono potersi riferire anche a banche dati costituite in ragione di un’attività di trattamento di dati personali connessa al funzionamento di un *whistleblowing scheme*.

Né parrebbero poter tenere il titolare di tale particolare trattamento esente dall’obbligo di notificazione le esenzioni oggetto dei successivi interventi chiarificatori del Garante. In particolare, con “Provvedimento a carattere generale” del 31 marzo 2004, il Garante ha specificato le tipologie di trattamenti di dati personali sottratti all’obbligo di notificazione ai sensi dell’art. 37, comma 1, d.lgs.

³⁶ Il Garante italiano potrebbe pronunciarsi verificando quanto già fatto in proposito dalla già citata autorità francese CNIL, la quale - dopo aver negato nel maggio 2005 a due società appartenenti a gruppi statunitensi (McDonald's France e CEAC/Exide Technologies) l’approvazione delle rispettive *hotlines* da implementare al fine di conformarsi alle Linee Guida SOX - ha stabilito che, ove l’adozione del *whistleblowing scheme* sia pienamente rispettosa dei principi stabiliti dalla menzionata *autorisation unique* dell’8 dicembre 2005, sarà sufficiente far pervenire alla CNIL una dichiarazione di *engagement de conformité*. Ove, diversamente, lo schema da implementare si discosti dalle Linee Guida dettate dalla suddetta autorizzazione generale, sarà necessario richiedere alla CNIL un’apposita autorizzazione *ad hoc*.

³⁷ Si ricorda che la materia delle “centrali rischi” è stata oggetto di importanti interventi ad opera del Garante per la protezione dei dati personali italiano, con l’emanazione del “Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti” e del provvedimento in tema di “Bilanciamento di interessi” (deliberazioni del 16 novembre 2004, n. 8 e 9).

196/2003. In esso si precisa che non sono soggetti all'obbligo di preventiva notificazione - con riferimento ai casi di cui alla lett. *f*) del comma 1 dell'art. 37 - i trattamenti di dati registrati in banche di dati utilizzate nei rapporti di fornitura di beni, prestazioni e/o servizi con l'interessato (tra i quali, dal successivo "Parere" del 23 aprile 2004 del medesimo Garante, sono espressamente menzionati assieme ai clienti e ai fornitori, anche i dipendenti), anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato, nonché i trattamenti di dati registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di lavoro, previdenza o assistenza, comprensivi (sempre secondo il suddetto "Parere" del 23 aprile 2004) di quelli concernenti eventuali obblighi derivanti dalla contrattazione collettiva.

(iv).d Ambiti soggettivo ed oggettivo di applicazione

La procedura dovrebbe altresì essere elaborata avendo cura di verificare se limitare il novero dei soggetti che possono avere accesso al *whistleblowing scheme* in qualità di *whistleblowers*, nonché il novero dei soggetti che possono essere segnalati attraverso i medesimi schemi, in ragione, ad esempio, delle rispettive specifiche funzioni e posizioni aziendali.

Al riguardo, il più elevato numero di circostanze potenzialmente passibili di segnalazione e le più ampie finalità cui tende l'implementazione dei *whistleblowing schemes* alle quali si è fatto cenno, rispetto ai Modelli di cui al d.lgs. 231/2001, tenderebbero a suggerire una loro applicazione senza limitazioni soggettive. Una simile scelta dovrebbe tuttavia accompagnarsi ad una chiara indicazione circa il tipo di informazioni che possono essere oggetto di segnalazione³⁸, dandosi così luogo al trattamento delle sole informazioni necessarie per l'effettuazione degli accertamenti ad esse strettamente connessi. Tale chiarezza andrebbe altresì a beneficio dei soggetti preposti, costituendo, pur nell'ambito dell'autonomia e dell'indipendenza che devono contraddistinguere l'operato, una valida bussola per orientarsi nella difficile attività di primo *screening* delle segnalazioni loro pervenute.

Analoghe considerazioni, nonché l'elevato grado di riservatezza con il quale dette segnalazioni (e l'identità dei rispettivi autori) dovranno essere trattate, farebbero propendere per una scelta che non preveda la possibilità di segnalazioni anonime. Oltremodo difficoltosa appare infatti, a giudizio di chi scrive, la previsione di eccezioni legittimanti *anonymous complaints*, in ragione delle diverse soglie emotive alle quali ciascun *whistleblower* farebbe appello.

³⁸ Sul punto l'autorità francese CNIL, così si esprime: "*Le champ du dispositif d'alerte est défini par l'employeur, dans le respect de l'article 1er de l'autorisation unique du 8 décembre 2005. En conséquence, seuls des faits se rapportant à des risques sérieux pour l'entreprise dans les domaines comptable, d'audit financier, de lutte contre la corruption ou bancaire peuvent être recueillis et enregistrés par l'organisation chargée de la gestion des alertes*". E ancora "*L'article 3 de l'autorisation unique permet également la prise en compte, dans le dispositif d'alerte, de faits ne relevant pas du champ du dispositif compte tenu de leur particulière gravité. Celle-ci est appréciée au cas par cas par l'organisation chargée de la gestion des alertes. Au sens de l'autorisation unique, sont considérés comme graves les faits mettant en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés*" (FAQ sur les dispositifs d'alerte professionnelle, n. 10).

(iv).e Ambito di conoscibilità del contenuto delle segnalazioni

Un ultimo aspetto riguarda l'eventuale comunicazione, all'esterno della società, dei dati personali raccolti nell'ambito delle segnalazioni pervenute, come potrebbe, ad esempio, rendersi necessario nei gruppi di società nei quali la gestione delle indagini successive alle segnalazioni dovessero essere svolte da un *team* maggiormente qualificato di cui disponesse soltanto la capogruppo (cd. *ethic officers*). Tale questione sarebbe ulteriormente complicata nel caso di capogruppo con sede in Stati diversi dall'Italia, in particolare *extra*-UE, con applicazione della disciplina dettata dall'art. 43 d.lgs. 196/2003.

Un accorgimento pratico per ovviare alla suddetta problematica potrebbe consistere nella trasformazione (temporanea) dei dati personali contenuti nelle segnalazioni in dati "anonimi" (secondo la definizione dell'art. 4, comma 1, lett. *n*), d.lgs. 196/2003), non associabili ad un interessato identificato o identificabile se non ad opera del soggetto preposto. L'eventuale "ri-personalizzazione" di tali dati potrebbe successivamente essere considerata a fronte di un più fondato e certo motivo che conduca la società e la capogruppo a decidere di far valere o difendere un diritto (individuale o di gruppo) in sede giudiziaria, operando in tal caso la legittimante di cui all'art. 43, comma 1, lett. *e*), d.lgs. 196/2003.

5. Conclusioni

L'esame sinora condotto fa ritenere che l'attuazione dei *whistleblowing schemes*, ove rispettosa dei principi sopra esposti, possa dirsi lecita. Appare infatti possibile introdurre procedure come quelle in esame, in ossequio dei principi di necessità, finalità, trasparenza, legittimità, proporzionalità ed accuratezza, necessari al fine di poter correttamente e positivamente esperire quel delicato processo di bilanciamento di interessi (o *balance of interest test*) di cui si è sinora scritto.

Ripercorrendo i punti salienti delle Linee Guida offerte dal Parere WP117, si ritiene che il motivo legittimante dei *whistleblowing schemes* possa essere individuato, prima ancora e piuttosto che in specifiche fonti normative, in prima battuta in una ragione di tutela dei patrimoni aziendali e, di riflesso e in un'ottica più ampia, dell'intero sistema economico nel quale detti patrimoni si collocano ed operano. Queste esigenze (*rectius* diritti e libertà) occupano, in un'ideale scala di valori, una posizione sufficientemente elevata per poter affrontare e sostenere quella prova di "resistenza" o di verifica di "parità di rango"³⁹ rispetto ad altri diritti e libertà fondamentali, necessarie nel momento in cui dette posizioni giuridiche, apparentemente antinomiche, si trovano ad interagire.

³⁹ Di particolare interesse, al fine di comprendere quale sia il modo corretto per valutare la sussistenza della "parità di rango" dei diversi diritti potenzialmente coinvolti, risulta il "Provvedimento generale sui diritti di pari rango" predisposto dal Garante in data 9 luglio 2003. Nello specifico, in detto documento il Garante chiarisce che nel valutare il "rango" del diritto che s'intenda difendere o far valere in giudizio, dev'essere utilizzato come parametro di raffronto non il "diritto di azione e difesa" in sé e per sé, quanto il "diritto sottostante" che s'intende così azionare. E' tale sottostante diritto che deve vincere il *test* della "parità di rango" rispetto al diritto che l'interessato ha di mantenere riservati i dati relativi, nella fattispecie, alla propria salute e/o vita sessuale.

E l'equivalenza di dignità di protezione dei suddetti diritti da parte dell'ordinamento può affermarsi non solo su di un piano "qualitativo" dei medesimi, ma altresì su di un piano "quantitativo", ossia di titolarità diffusa e generale degli stessi. Nella fattispecie in esame, ad esempio, ai diritti e alle libertà attinenti alla sfera della riservatezza dei soggetti coinvolti nell'attuazione dei *whistleblowing schemes*, si contrappongono i diritti e le libertà propri degli *shareholders* e, ancor più, degli *stakeholders* che a vario titolo interagiscono con la società. Appare evidente come a questi ultimi non si possa negare la fondatezza dell'interesse a che la società nella quale e/o per la quale essi operano sia dotata di ogni strumento che lecitamente si dimostri idoneo a tutelarne l'integrità patrimoniale.

Dovrebbe essere altrettanto chiaro che, verificata nei termini sopra accennati la fonte legittimante dei *whistleblowing schemes*, non possa tuttavia prescindere dalle modalità di concreta loro introduzione ed attuazione nelle realtà societarie italiane. Ciascun *whistleblowing scheme* dovrà essere infatti elaborato e attuato avendo specificamente individuato i soggetti, i mezzi, i luoghi e le procedure attraverso i quali lo schema sia in grado di funzionare e, comunque, nel rispetto dei già menzionati principi di qualità e proporzionalità dei dati trattati, "trasparenza" nell'adozione e nell'applicazione delle procedure, rispetto dei diritti dei soggetti segnalati, sicurezza dei sistemi di trattamento dei dati e corretta gestione delle procedure.

Risolte in senso positivo, almeno in via astratta, le questioni di ordine giuridico alle quali si è sinora fatto cenno - e, *de iure condendo*, in attesa di specifiche normative *ad hoc* e/o di Linee Guida fornite dalle competenti autorità (tra le quali, si è scritto, certamente il Garante per la protezione dei dati personali) capaci di "sdoganare" dette procedure - risulta comunque assai arduo pronosticare l'utilizzo effettivo dei *whistleblowing schemes* nel contesto societario italiano.

Ciò che rende tale previsione particolarmente difficile da compiere è l'assoluta assenza di esperienze in tal senso nel panorama nazionale (ad esclusione dei più "limitati" Modelli di Organizzazione e di Gestione ai sensi del d.lgs. 231/2001), addirittura desolante se messo a confronto con il mondo statunitense nel quale tali procedure sono a tal punto note ed utilizzate da aver portato alla nascita di organizzazioni che offrono specifici programmi a supporto, anche finanziario, dei *whistleblowers*⁴⁰.

Viene spontaneo chiedersi, insomma, se la presenza ed il funzionamento di tali procedure avesse potuto scongiurare in Italia l'accadere dei recenti scandali finanziari (o limitarne, quantomeno, le conseguenze socio-economiche grazie ad una loro più repentina scoperta), come in effetti avvenuto negli USA⁴¹.

Evidentemente, le risposte ai suddetti quesiti potranno soltanto essere date *a posteriori*, analizzando i risultati dei primi *whistleblowing schemes* che saranno attuati

⁴⁰ Il riferimento è al *Whistleblower Support Network*, un programma di supporto di iniziativa dell'organizzazione senza scopo di lucro denominata GAP (*Government Accountability Project*), con sede a Washington DC, il cui obiettivo "is to allow individuals who are considering blowing the whistle, or already have done so, to contact former whistleblowers to seek confidential advice, guidance, or simply to share what they are going through. Often for new whistleblowers, it helps tremendously to speak directly with someone who has gone through a similar situation. Conversely, individuals who have gone through this taxing process are often interested in sharing their experiences; they can offer key advice and answer burning questions from those in need" (www.whistleblower.org).

⁴¹ Si pensi, ad esempio, alla vicenda che ha visto protagonista la dipendente della società statunitense Enron, Sherron Watkins, nominata dalla rivista *Time* "Woman of the year, 2002", per aver contribuito a portare alla luce i comportamenti illeciti dell'allora presidente e CEO Enron, Kenneth Lay.

nelle realtà societarie italiane. Sin d'ora può però ribadirsi che evidente appare la tendenza dell'ordinamento italiano, analogamente a quanto già accade a livello internazionale, alla creazione di un complesso ma organico sistema di *control governance*, di carattere prevalentemente (anche se non esclusivamente) endosocietario, il cui fine è rappresentato dal potenziamento delle funzioni proprie degli organi amministrativi, dei collegi sindacali e dei revisori esterni. L'intento ultimo è quello di far sì che le società si dotino di adeguati meccanismi di difesa - o "forme di controllo endogene al sistema"⁴² - in grado di segnalare con tempestività (se non, addirittura, evitare) il compimento di attività fraudolente, anche a supporto dell'attività di vigilanza svolta dagli organismi pubblici.

La suddetta evoluzione offre certamente lo spunto - come scritto da Assonime riferendosi alla propria Circolare n. 45/2006 nella quale si approfondisce il rapporto tra le nuove norme penali sui reati di abuso di informazioni privilegiate (art. 184 d.lgs. 58/1998) e di manipolazione del mercato (art. 185 d.lgs. 58/1998) e la disciplina sulla responsabilità amministrativa degli enti dettata dal d.lgs. 231/2001 - "per una più ampia riflessione sull'efficacia di alcune soluzioni tecniche adottate nella legislazione d'impresa degli ultimi anni, che si caratterizza per un'idea di sana e corretta gestione dell'impresa realizzata mediante un'efficiente organizzazione aziendale. Sembra infatti affermarsi una politica di prevenzione degli illeciti attuata anche attraverso la predisposizione di procedure aziendali di controllo che consentano di monitorare gli atti rilevanti dell'attività d'impresa e di individuare soggetti responsabili delle singole fasi del procedimento".

Sia consentita un'ultima notazione. Alle voci di coloro che temono possibili "crisi di rigetto" da parte degli organismi societari nei quali siano innestati troppi e troppo repentinamente elementi (fatti di procedure e soggetti alla stregua di quelli descritti) ad essi sinora estranei, soprattutto in ragione della circostanza che a questi si guardi come centri di costo, lontani dal vero e proprio ciclo produttivo aziendale, pare legittimo replicare che l'unica efficace "terapia" consista nell'accompagnare detti interventi ad un'evoluzione di carattere culturale originante da una ferma e chiara volontà espressa in tal senso da parte dei vertici aziendali, i quali dovranno farsi promotori con il *management* e l'organico dei dipendenti di una costante (e coerente) attività di *moral suasion*⁴³.

⁴² Queste le parole utilizzate dal presidente CONSOB, Lamberto Cardia, rivolgendosi al mercato finanziario nella Relazione per l'anno 2003, pp. 4 ss...

⁴³ Di particolare interesse risultano in proposito le affermazioni di G. CAPECCHI, *op cit.*, p. 117, secondo il quale l'"attività di informazione e formazione" che deve necessariamente accompagnare l'adozione di qualsiasi codice di condotta "dovrà inoltre prefiggersi uno scopo ancora più ambizioso che richiede, per essere raggiunto, un'abile capacità di gestione delle risorse umane: convincere i dipendenti della serietà dell'ente nel ripudiare condotte criminogene. Solo in questo modo, infatti, potrà attivarsi un circolo virtuoso che vedrà i dipendenti non soltanto evitare comportamenti vietati ma segnalare all'ente (e, per esso, al suo Organismo di Vigilanza) le attività sospette con cui, inevitabilmente, i dipendenti verranno a contatto nel corso della loro vita professionale". Evidenzia con chiarezza come il contesto organizzativo di riferimento rilevi maggiormente rispetto alle stesse caratteristiche personali del *whistleblower* (ossia, profilo demografico - età anagrafica e anzianità di servizio, livello di istruzione, sesso - profilo etico e posizione lavorativa), C. FLORIO, *op. cit.*, p. 939, la quale rileva che "il *whistleblowing* è più frequente nei contesti organizzativi in cui i *whistleblowers* percepiscono una maggiore congruenza tra valori personali e valori dell'organizzazione".