Circolare 231

approfondimenti, notizie e informazioni

n. 6 - giugno 2015

PLENUM

rivista231.it

Sommario

AMBIENTE E SICUREZZA

di Marina Zalin, Butti & Partners, Verona

Omicidio colposo commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Il Tribunale di Trento, con una sentenza dello scorso 18 marzo 2015, ha preso una netta posizione in tema di responsabilità amministrativa dell'ente per il reato di omicidio colposo con violazione delle norme antinfortunistiche, sancita dall'art. 25-septies D.Lgs. 231/2001 con sanzioni di natura pecuniaria e interdittiva.

Nel caso di specie il Tribunale tridentino si sofferma sul legame tra "reati presupposto" di matrice colposa, quale quello considerato, e la responsabilità dell'ente che è punibile solo se vi è un'intenzione chiara di perseguire, per il tramite della commissione del reato, un interesse o vantaggio in favore dell'ente stesso.
Una condotta colposa commessa dalla persona fisica può costituire presupposto di responsabilità per l'ente solo nella misura in cui si riscontri, in capo a quest'ultimo, un consapevole e doloso conseguimento di un interesse o vantaggio (anche di natura "negativa", in termini di risparmio).
Il ragionamento muove i passi dalla pronuncia delle Sezione Unite, resa il 24 aprile 2014 con sentenza n. 38343, che distingue come identificare le nozioni di "interesse" e "vantaggio" per quanto concerne la posizione dell'ente.
Interesse e vantaggio sarebbero elementi presupposto, per l'applicazione della normativa, che possono essere riscontrati in via alternativa e concorrente: in particolare l'interesse rappresenterebbe una "valutazione teleologica del reato" apprezzabile in prospettiva soggettiva ed ex ante, mentre il vantaggio andrebbe identificato con gli effetti prodotti, valutati in prospettiva oggettiva ed ex post.
Ciò non significa, tuttavia, che la consapevolezza della coscienza e volontà del fine di "interesse o vantaggio" possa essere elisa o ritenuta non necessaria in ragione del fatto che il "vantaggio" potrebbe essere identificato proprio a valle della commissione del reato.
Il Tribunale sottolinea che il caso posto all'esame delle Sezioni Unite era relativo a reati-presupposto coperti dall'elemento del dolo eventuale, dichiaratamente e pacificamente preordinati al risparmio di costi in materia di sicurezza sul lavoro.

La diversità degli elementi di fatto su cui poggiano le decisioni in punto di diritto, pertanto, consente di ritenere che la struttura dell'illecito amministrativo dipendente da reato, richiamando Cassazione Penale n.25483/2010, si estrinsechi in tre elementi costitutivi: la commissione di un reato-presupposto, il rapporto qualificato di relazione tra il reo e l'ente e l'interesse o vantaggio per l'ente a fronte del reato.

Nel caso di specie, ad avviso del Tribunale, il Pubblico Ministero si è limitato a proporre considerazioni presuntive per dimostrare la sussistenza di interesse e/o vantaggio per l'ente (consistente in risparmio economico per la mancata adozione di presidi antinfortunistici).
L'accusa, infatti, avrebbe inteso legare in modo inequivoco il mancato compimento dell'azione doverosa e il conseguente risparmio economico, identificando così l'interesse o vantaggio per l'ente: il risparmio, in altre parole, sarebbe il fine ultimo della mancata adozione di quanto dovuto.
Nel caso in esame l'ente aveva commissionato a un esperto la redazione del Documento di Valutazione dei Rischi (DVR), prestazione professionale senz'altro onerosa, il quale aveva però omesso di valutare i "rischi da interferenze" con le altre ditte nel c.d. DUVRI.
Il Pubblico Ministero segnala come il costo reale della redazione del documento non potesse avere valore superiore ai 250-700 euro, ma le prescrizioni ivi contenute avrebbero comportato esborsi complessivi superiori a 20.000 euro (per gli stabilimenti del gruppo aziendale).
Il Tribunale, tuttavia, ha ritenuto che il ragionamento non potesse trovare accoglimento proprio perché tale seconda – e ben maggiore – voce di costo rappresenterebbe qualcosa di "ignoto" per l'ente, il quale mai sarebbe stato posto nella condizione di valutarla.
Il vantaggio potrebbe essere identificato solo in qualcosa di effettiva conoscenza e consapevolezza dell'ente, che nel caso di specie ha scientemente "risparmiato " solo il costo della redazione del DUVRI e non, anche, delle successive installazioni.

Diverso sarebbe stato il caso, ad avviso del Giudice, ove il documento fosse stato redatto ma le prescrizioni non fossero state ottemperate: solo in quel caso, a questo tuttavia non affine, si sarebbe potuto quantificare il risparmio economico in modo diretto secondo la tesi accusatoria.
"Non si può neppure parlare di una scelta di risparmio di spese" dice il Tribunale "dovute alla mancata installazione d'impianti di sicurezza che nessuno in concreto ha proposto, e che quindi non sono stati mai neppure presi in considerazione".
La responsabilità dell'ente non può pertanto essere provata solo in ragione della colposa omissione ad opera di una o più delle persone fisiche ai

vertici dell'ente, ma serve un nesso finalistico con lo scopo di una volontaria - o quantomeno consapevole - scelta di risparmio aziendale in materia di sicurezza.
Risparmio che, a ben vedere, deve essere quantitativamente apprezzabile e non può essere presuntivamente valutato sulla base di mere deduzioni postume effettuate dagli organi inquirenti, ma deve essere invece stato previamente conosciuto o conoscibile da parte dell'ente, che ne ha soppesato l'entità e ha scelto così di perseguirlo.

ANTIRICICLAGGIO (1)

di Ranieri Razzante, Docente di Intermediazione finanziaria e Legislazione Antiriciclaggio presso l'Università di Bologna

Una nuova Direttiva contro il riciclaggio

È stata pubblicata nella Gazzetta Ufficiale dell'Unione europea la Quarta Direttiva antiriciclaggio.
A distanza di dieci anni dall'ultima revisione delle norme europee relative alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e del finanziamento del terrorismo, la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.
Frutto di intense negoziazioni, la Quarta Direttiva - presentata dalla Commissione nel febbraio del 2013 – costituisce senza alcun dubbio un importante risultato nel quadro europeo antiriciclaggio. Ciò in quanto non solo dà attuazione alle Raccomandazioni FATF (Financial Action Task Force), allineando in tal modo i Paesi Ue ai più avanzati standard internazionali, ma introduce una serie di disposizioni fondamentali che consentiranno all'Europa di compiere passi avanti nel contrasto al riciclaggio e al finanziamento del terrorismo.

In tal senso, la normativa approvata – allo scopo di accrescere la trasparenza in merito alla proprietà delle società e dei trust, nonché di fornire alle autorità strumenti efficaci per la lotta al riciclaggio e al finanziamento del terrorismo – introduce in tutti i Paese appartenenti alla Ue un registro centralizzato di informazioni riguardo alla proprietà effettiva. Pertanto, entro il mese di giugno del 2017, i Paesi aderenti dovranno dotarsi di un registro centrale che conterrà i dati sui beneficiari di fondi fiduciari e altro strumenti finanziari, sulle transazioni di alto valore e altre informazioni sensibili. Detto registro sarà accessibile non solo alle autorità competenti nazionali ed europee, ma anche a chi dimostra di avere un interesse legittimo ad ottenere tali informazioni; "legittimo interesse" che certamente necessiterà di ulteriori chiarimenti.
Inoltre, la nuova Direttiva – consapevole dell'importanza dell'adozione di un approccio sovranazionale in relazione al rischio di riciclaggio – affida alla

Commissione europea il compito di condurre una valutazione sovranazionale di tale rischio e di formulare raccomandazioni agli Stati membri affinché questi possano farvi fronte in maniera adeguata. Così, da un lato, verranno irrigiditi gli obblighi di monitoraggio su persone considerate a rischio di corruzione e su determinati settori economici e, dall'altro, saranno dettate procedure semplificate per chi presenta un basso rischio di riciclaggio. Disposizioni queste che, tuttavia, non rappresentano per il nostro Paese un vero stravolgimento, considerato che la normativa vigente già è uniformata in tal senso.
Ulteriori disposizioni sono state invece dedicate alla tracciabilità del trasferimento di fondi, ritenuta di particolare importanza per la prevenzione, individuazione ed accertamento di condotte di riciclaggio o finanziamento del terrorismo. A differenza dell'attuale regolamentazione, che già obbliga i fornitori di servizi di pagamento a richiedere informazioni sull'ordinante, il nuovo testo prevede la raccolta di informazioni anche sul beneficiario.

Secondo la nuova Direttiva, l'Autorità Centrale delle Banche Europee, l'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali nonché l'Autorità Europea sugli strumenti finanziari e sui mercati saranno chiamate ad emanare linee guida sui requisiti e modalità per poter effettuare il trasferimento di fondi anche in ipotesi di informazioni mancanti o incomplete sul pagatore o beneficiario.
In ultimo, sono state introdotte innovazioni relative alle sanzioni volte a rafforzare la conformità. La nuova Direttiva prevede una sanzione pecuniaria pari al doppio dell'ammontare del beneficio derivante dalla violazione ovvero di almeno un milione di euro. Per le violazioni che coinvolgono enti creditizi o finanziari nei casi di persone giuridiche, una sanzione pecuniaria massima di almeno cinque milioni di euro ovvero del dieci percento del fatturato annuo totale dell'esercizio precedente; nel caso di persone fisiche, invece, è prevista una sanzione pecuniaria di almeno 5 milioni di euro ovvero il doppio del profitto ricavato o le perdite evitate grazie alla violazione, quando questi possono essere determinanti.

ANTIRICICLAGGIO (2)

di Sandro Bartolomucci, avvocato, partner di LS Lexjus-Sinacta

L'intervento di aggiornamento dei modelli 231 al nuovo reato di autoriciclaggio: un approccio realistico

Superato lo scoglio dogmatico del "ne bis in idem", il Legislatore con la legge n. 186/2014 ha introdotto con l'art. 648-ter 1 c.p. il nuovo delitto di Autoriciclaggio.
Non ci soffermeremo, in questa sintetica riflessione, sui caratteri e i contenuti della norma, già ampiamente approfonditi nei precedenti numeri della Circolare 231. Sarà sufficiente ricordare che si tratta di un reato proprio (l'autore è individuabile per relationem rispetto alla commissione o al concorso nella commissione del reato-fonte), pluri-offensivo e caratterizzato da dolo generico. La norma (volutamente) non definisce un numerus clausus di reati-fonte, rispetto ai cui proventi illeciti venga realizzata la condotta tipica di re-immissione nel circuito economico lecito con concreto ostacolo alla loro identificazione. Condotta che configura un reato autonomo e non un "post factum". Conseguentemente, spetta all'operatore effettuare una ricognizione dei possibili delitti che, nel proprio contesto aziendale ed operativo, possano costituire il presupposto necessario della successiva azione di money laundering.

Il dettato normativo non è privo di opacità lessicali, di aspetti problematici e di un deficit di dosimetria edittale, operata in funzione della gravità del reato-fonte. Un discorso a parte merita l'ermeneusi del 4° alinea, che considera il godimento personale dei proventi illeciti quale causa esimente da punibilità. Prescrizione che sta alimentando un dibattito dottrinario tra chi la considera superflua e ripetitiva, chi la sminuisce ad ipotesi di applicazione residuale ("Fuori dei casi di cui ai commi precedenti") e quanti la ritengono provvidenziale contenimento dell'afflittività della fattispecie ordinaria del 1° comma. In ogni caso, c'è da presumere che costituirà l'"exit strategy" privilegiata in sede difensiva.
L'impatto che la novella legislativa può produrre - amplificato dall'art. 3, 5° comma che dispone l'inserimento del reato de quo nel Catalogo dei reati-presupposto ex D.Lgs. n. 231/2001 - è importante per una serie di ragioni. Ne consegue la legittima preoccupazione di quanti intendano integrare i propri Compliance programs con strumenti di prevenzione di tale reato.

Certo, il testo normativo non aiuta: alcuni elementi del paradigma presentano un significato incerto; appare articolata e complessa la condotta criminosa richiesta; difetta la tipizzazione del reato a monte.
Lo stato di incertezza - invero, superabile solo col futuro vaglio giurisprudenziale - sta dando la stura a letture diremmo "stressogene" da parte dei primi commentatori, che raccomandano verifiche analitiche e omnicomprensive di ogni possibile potenzialità di reato, nonché l'attivazione di strumenti special-preventivi "a pioggia".
Va altresì registrata la posizione di talune lobby, ieri contrarie all'introduzione dell'art. 648-ter 1 c.p., oggi preoccupate dal paventato rischio di excessive control.
A nostro parere è praticabile una ermeneusi della norma che, senza essere minimalista, valorizzi alcuni importanti fattori di rilievo pratico-applicativo.
Partiamo dalla collazione dei testi degli articoli 648 bis e 648 ter 1 c.p..
Appare evidente, al netto del superamento della c.d. "clausola di riserva" e dei connotati dell'articolata e qualificata condotta richiesta per realizzare l'autoriciclaggio, che le due fattispecie presentano un costrutto, se non perfettamente sovrapponibile, certamente equivalente.

Di talché, quanti abbiano già implementato un MOG dotato di una sezione dedicata al preesistente art. 25-octies, potranno agevolmente integrarla, orientando l'azione prevenzionale anche al reimpiego dei proventi illeciti non ad opera di un soggetto terzo (riciclatore), bensì in self-laundering.
Mette conto, poi, di ricordare che il dettato dell'art. 6, comma 2, lett. c) del D.Lgs. n. 231 raccomanda da sempre la definizione delle "modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati".
Nell'intervento di aggiornamento del MOG in chiave anti-autoriciclaggio, certamente il baricentro risulta costituito dalla mappatura delle potenzialità commissive. Il censimento e la ponderazione di tali rischiosità impone, a monte, l'identificazione delle potenzialità commissive del reato-fonte, il cui provento illecito possa essere reimpiegato ad opera dell'autore (o del concorrente).
Operazione dalle considerevoli ricadute pratiche, stante l'omessa tipizzazione legislativa del reato-fonte, di cui viene solo dichiarata la natura non colposa. Permettendo, comunque, di liberare il campo dalle ipotesi di contravvenzione e di delitto colposo.

Orbene, riteniamo che l'Assessment di tali rischiosità non possa pretendere il checking analitico ed esaustivo di ciascuna fattispecie ricompresa nel Codice penale (nemo ad impossibilia tenetur…). Neanche limitando il range della verifica alle sole fattispecie ipotizzabili sulla scorta dei connotati identificativi e peculiari dell'ente empirico (i.e. forma giuridica, linea di business, assetto di governance, aspetti dimensionale ed operativo, ecc.).
Una sorta di tipizzazione ab externo delle specie di reato-fonte va comunque profilandosi.
L'ipotesi più "gettonata" risulta il reato tributario (che resta estraneo al Catalogo 231, in ossequio al principio di legalità dell'art. 2 del decreto), nonostante le problematiche ermeneutiche connesse al distinguo tra "ricavo illecito"e semplice "risparmio d'imposta".
Ma le fattispecie criminogene rispetto all'autoriciclaggio restano numerose.
Muovendo dal numerus clausus 231, potremmo citare le false comunicazioni sociali (art. 25-ter); la truffa ai danni dello Stato e la corruzione (artt. 24 e 25); i delitti ambientali (art. 25-undecies); la contraffazione di marchi e segni distintivi (art. 25-bis); il market abuse (art. 25-sexies); le violazioni del diritto d'autore (art. 25-novies).
Elenco destinato a subire un'automatica espansione allorché il Legislatore integrerà il catalogo con nuovi reati (non colposi).
Sul fronte codicistico, le fattispecie (non rilevanti ex 231) sono a mò d'esempio i reati doganali, quelli fallimentari, l'appropriazione indebita, oltre al già evocato reato tributario.

In ogni caso, valga evidenziare che l'Assessment rispetto all'art. 648-ter 1, oltre a dover considerare le concrete caratteristiche dell'ente empirico, dovrà accertare la ricorrenza delle condizioni di imputabilità dell'ente collettivo. Pertanto, a prescindere dalla tipologia di reato-fonte, l'autoriciclaggio potrà generare l'illecito dell'ente solo qualora sia contestabile un suo deficit organizzativo e le condotte tipizzate dalla norma vengano realizzate da un soggetto organico, nell'interesse/vantaggio della societas.
Eppoi, quand'anche l'impegnativo screening di ciascuna tipologia di reato-fonte non fosse praticabile, ovvero risultasse non esaustivo, l'azione cautelare ex 648-ter 1 potrà essere focalizzata sull'altra condotta co-essenziale alla realizzazione dell'autoriciclaggio: l'azione di ostacolo (causalmente efficiente) all'identificazione della provenienza delittuosa dei proventi del (primo) reato.

E passiamo, appunto, all'altra operazione richiesta per l'aggiornamento del Compliance Program al delitto di autoriciclaggio: l'elaborazione dei Protocolli Speciali.
Siamo dell'avviso che tale operazione non comporti soverchie difficoltà.
Intanto, un supporto in chiave special-preventiva potrà derivare dai Modelli 231 vigenti.
Pensiamo, a tacer d'altro, alle sezioni volte a prevenire i Reati nei confronti della P.A. (art. 25), sub species della Corruzione attiva.
E' evidente che il contrasto ai comportamenti corruttivi verso esponenti pubblici (o soggetti privati), si estrinsechi nell'impedire la costituzione e l'utilizzo da parte dell'ente di fondi extra-contabili, disponibilità queste frutto, appunto, della commissione di un reato-fonte.
Ulteriori cautele - di più ampia portata, giacché destinate a prevenire non solo reati, quanto manifestazioni di mala administration - potranno risultare dai Piani Anticorruzione ex l. n. 190/2012 c.s.m. (coordinati al MOG), elaborati ad es. dagli "organismi privati in controllo pubblico" che risultino espressamente assoggettati alla normativa del c.d. "Pacchetto Anticorruzione", ovvero lo siano in virtù dell'interpretazione "inclusiva" datane dall'ANAC.

Preziose indicazioni vengono offerte anche dalle Linee guida di Confindustria (aggiornate al marzo 2014), sebbene le misure in esse suggerite si riferiscano alla prevenzione del reato di riciclaggio (art. 648-bis). Ciò nondimeno, rivestono attitudine cautelare anche rispetto all'autoriciclaggio: la verifica della provenienza delle somme di denaro; la selezione dei fornitori di beni e di servizi e dei partners; la tracciabilità e trasparenza contabile; la segregazione delle funzioni/responsabilità nella gestione di determinati processi; la tenuta di rapporti con taluni soggetti; la definizione dei poteri autorizzativi per gli investimenti; la verifica delle motivazioni e condizioni delle operazioni di straordinaria amministrazione.
Nelle organizzazioni complesse, come i Gruppi societari - ancor più se multinazionali – concorreranno all'azione prevenzionale anche i tipici presidi, come la definizione della Policy del transfer price, il monitoring dell'erogazione dei servizi infra-gruppo, la politica degli investimenti, la disciplina degli accordi di joint ventures.
Oltre alle istruzioni delle Associazioni categoriali di rilevanza nazionale, un autorevole supporto tecnico è atteso dal Ministero della Giustizia, sentita l'Unità di Informazione Finanziaria, a mente dell'art. 25 octies, 3° alinea.

Da ultimo, seppur circoscritto ad un ambito settoriale, riteniamo che l'aggiornamento in parola sia agevolato rispetto all'ampia categoria dei destinatari del D.Lgs. n. 231/2007.
Trattasi degli Intermediari finanziari e degli eterogenei soggetti (artt. 10-14) che già utilizzano MOG conformati alle prescrizioni del decreto del 2007 (i.e. adeguata verifica della clientela, identificazione delle operazioni sospette, ecc.), alle istruzioni impartite dalle Authority e alla normativa regolamentare.
In conclusione, siamo dell'avviso che i molteplici fattori (interpretativi e di supporto applicativo) qui solo richiamati, se non qualificano come minimalista il restyling dei Modelli "231" a presidio del rischio di autoriciclaggio, suggeriscano una lettura realistica e rassicurante della norma a quanti debbano cimentarsi nella "ardua impresa".

GIURISPRUDENZA ANNOTATA

di Ciro Santoriello, Sostituto Procuratore presso il Tribunale di Torino

Costituzione dell'ente ed esercizio del diritto di difesa

La decisione

Sequestro preventivo – Procedimento di riesame – Richiesta di riesame avanzata dal difensore di fiducia della persona giuridica in assenza di una formale costituzione dell'ente – Ammissibilità (C.p.p., artt. 321, 324; D.lg. n. 231 del 2001, art. 39, 52, 53, 57)

Nell'ambito del processo verso un ente collettivo per la sua responsabilità da reato, deve ritenersi ammissibile la richiesta di riesame avverso il decreto di sequestro preventivo proposta dal difensore di fiducia dell'ente, pur in assenza di un previo atto formale di costituzione a norma dell'art. 39 d.lg. n. 231 del 2001 (1).

CASSAZIONE PENALE – SEZIONI UNITE – C.C. 28 MAGGIO 2015, N. 15249, IN ATTESA DI DEPOSITO – SANTACROCE, PRESIDENTE – COVALM BIOGAS

(1) 1. La particolare rilevanza ed importanza della questione decisa dalle Sezioni Unite induce a dare immediatamente notizia del deposito del dispositivo, pur in mancanza della relativa motivazione.

2. Si ricorda che la costituzione della società deve avvenire secondo le modalità indicate nell'art. 39, il quale prevede che la persona giuridica interviene in giudizio con il proprio rappresentante legale quale risulta dalla legge o dallo statuto societario: in caso di mancata costituzione, ne viene invece dichiarata la contumacia conformemente ai principi generali del processo penale.
La dichiarazione di costituzione va presentata nella cancelleria o segreteria dell'autorità giudiziaria che procede e deve contenere le medesime indicazioni richiamate dall'art. 84 c.p.p.. In particolare, è prevista l'indicazione della denominazione dell'ente e delle generalità del legale rappresentante dello stesso; in secondo luogo, va effettuata la nomina del difensore – di cui va trascritto il nome ed il cognome –, il quale a sua volta

deve sottoscrivere l'atto e deve essere munito di apposita procura ad litem, essendosi per tale profilo parificata la posizione della persona giuridica interveniente nel processo penale che la riguarda a quella del convenuto nel giudizio civile; infine, occorre anche l'indicazione o l'elezione di domicilio della società e l'assenza di tali elementi determina – in assoluta divergenza rispetto a quanto previsto per le posizioni dell'imputato e delle altri private – l'inammissibilità della costituzione.
La mancanza di uno dei requisiti indicati nel citato art. 39, comma 2, lett. a), b), c) e d), determina l'inammissibilità della dichiarazione di costituzione: ovviamente nulla esclude che la dichiarazione inammissibile possa essere rinnovata eliminando i precedenti vizi, posto che non è previsto alcun termine per la costituzione dell'ente nel processo.
Va precisato che la disciplina in discorso – ed in particolare la normativa in tema di dichiarazione o elezione di domicilio - opera solo laddove la persona giuridica intenda costituirsi nel procedimento; allorquando invece l'ente non proceda alla costituzione saranno applicabili – secondo il dettato degli artt. 34 e 35 D.Lgs. n. 231 – le ordinarie norme processuali del codice di rito, e l'elezione o dichiarazione di domicilio andrà effettuata nelle forme di cui all'art. 162 c.p.p..

3. Particolarmente discusse sono le conseguenze che si ritiene debbano derivare nel caso di mancata costituzione dell'ente, con particolare riferimento alle facoltà difensive che la persona giuridica può esercitare in caso di omessa osservanza delle formalità di cui all'art. 39 citato.
Sul punto, si confrontano due diversi orientamenti giurisprudenziali diametralmente opposti, giacché mentre secondo Cass., sez. VI, 5 febbraio 2008, S.r.l. A.R.I. INTERNATIONAL (in Cass. Pen., 2009, 3799; nello stesso senso, Cass., sez. IV, 19 dicembre 2014, n. 3786, VB101) "l'esercizio dei diritti di difesa da parte dell'ente in qualsiasi fase del procedimento a suo carico è subordinato all'atto formale di costituzione a norma dell'art. 39, essendo dunque legittima l'ordinanza del tribunale della libertà che dichiari inammissibile la richiesta di riesame avverso un decreto di sequestro presentata dal difensore dell'ente non ancora costituitosi nel procedimento", con un'altra decisione (Cass, sez. VI, 5 novembre 2007, QUISQUEYANA, in Foro It., 2009, II, c. 37. Nello stesso senso, Cass., sez. VI, 23 giugno 2006, n. 32627, inedita) la medesima Cassazione ha sostenuto che "l'esercizio del diritto di difesa da parte della persona giuridica non è subordinato all'atto formale di costituzione e l'ente, non appena venuto a conoscenza dell'instaurazione di un procedimento a

proprio carico, non solo ha la facoltà di nominare nei modi previsti dall'art. 96 c.p.p., alla stregua di ogni altra persona sottoposta alle indagini o imputata, un difensore di fiducia, ma gode ovviamente del diritto di fruire dell'assistenza difensiva (ivi comprese le facoltà che il nostro codice riconosce al difensore) indipendentemente dall'atto formale di costituzione posto in essere a norma dell'art. 39".

4. In attesa delle motivazioni della decisione, ribadiamo che ritenere la costituzione dell'ente quale necessario presupposto per l'esercizio delle sue prerogative difensive confonde le condizioni richieste dal testo normativo perché la società possa partecipare al giudizio con il rispetto dei diritti che indefettibilmente spettano ad ogni accusato nel processo penale.
Infatti, mentre l'art. 39 D.Lgs. 231/2001 ha la funzione di "materializzare" l'ente nel processo con la sola conseguenza che in caso di inosservanza delle relative prescrizioni ne viene dichiarata la contumacia, i diritti di difesa riconosciuti ed esercitabili dalla persona giuridica vanno individuati e ricostruiti per il tramite del combinato disposto degli artt. 34 e 35 D.Lgs. n.231, i quale come è noto estendono le regole del processo ordinario, ed in particolare quelle riservate ai diritti e alle facoltà dell'imputato, all'ente "imputato" o sottoposto ad indagini preliminari. Indicativo di tale ricostruzione è il contenuto dell'art. 40 D.Lgs. 231 del 2001, che prevede la nomina del difensore d'ufficio all'ente che non ha nominato un difensore di fiducia o ne è rimasto privo: tale disposizione, infatti, pur potendo "sembrare ultronea rispetto al principio di parificazione tra imputato ed ente previsto dall'art. 35, ha una particolare valenza sistematica nella soluzione della questione in esame [proprio perché] garantisce la difesa dell'ente a prescindere dalla sua costituzione e la stessa locuzione utilizzata ha come soggetto l'ente e non l'ente "costituito"".

Misure cautelari

La decisione

Reati societari - Responsabilità amministrativa degli enti - Omicidio colposo o lesioni gravi o gravissime colpose con violazione delle norme sulla tutela della salute e sicurezza sul lavoro - Responsabilità dell'ente - Presupposti - Interesse o vantaggio - Apprezzamento - Contenuto - Fattispecie (D.Lgs. 8 giugno 2001 n. 231, articoli 5 e 25-septies)

In tema di responsabilità da reato dell'ente in conseguenza della commissione dei reati di omicidio colposo o di lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, la sussistenza dell'interesse o vantaggio per l'ente derivante dalle omissioni contestate all'autore del reato presupposto è congruamente argomentata con riferimento al consistente risparmio di costi per l'ente (1).

CASSAZIONE PENALE – SEZIONE QUARTA – 29 APRILE 2015 (C.C. 19 FEBBRAIO 2015), N. 18073 – BRUSCO, PRESIDENTE – IANNELLO, ESTENSORE – GALLI, P.M. (CONF.) – BARTOLONI.

(1) 1. La massima non presenta profili di novità, ribadendo sostanzialmente quanto chiaramente affermato dalle Sezioni Unite con la decisione del 15 settembre 2014 n. 37122 relativa alla drammatica vicenda Thyssen.
In quell'occasione venne esaminata la possibilità di rinvenire in capo all'ente un profitto economico maturato e derivante dalla commissione di un reato colposo, sostenendosi che il beneficio che il reo trae dalla sua condotta delittuosa non debba necessariamente tradursi in un accrescimento materiale del suo patrimonio – insomma non è necessario che in conseguenza del reato il responsabile dello stesso acquisisca la disponibilità di beni o somme di denaro, ulteriori rispetto a quello di cui era già in possesso -, giacché il profitto del crimine è nozione comprensiva anche di qualsivoglia utilità che il criminale realizza come effetto anche mediato ed indiretto della sua attività criminosa (Cass., sez. un., 25 ottobre 2007, Miragliotta, in Mass. Uff., n. 238700. Nello stesso senso, con

riferimento agli illeciti tributari Cass., sez. un., 30 gennaio 2014, Gubert, in Mass. Uff., n. 258647).

Sulla scorta di queste riflessioni diventa agevole riconoscere che nulla preclude la possibilità di rinvenire un profitto anche in presenza di reati colposi, ed in specie laddove la condotta colposa si concreti nella violazione della normativa sulla sicurezza sui luoghi di lavoro. In tale ipotesi, infatti, il profitto può individuarsi, quanto meno, nel risparmio di spesa inerente l'ammodernamento e la messa a norma degli impianti e più in generale la mancata adozione delle doverose misure di sicurezza e prevenzione degli infortuni e malattie professionali – dovendosi poi considerare, accanto a tale profilo, anche il beneficio pervenuto in capo alla società dalla prosecuzione dell'attività funzionale alla strategia aziendale ma non conforme ai canoni di sicurezza.

Si noti che questa conclusione è aderente a quanto asserito dalle Sezioni Unite nella principale decisione che si è occupata della definizione del profitto del reato con riferimento alla responsabilità da reato delle persone fisiche (Cass., sez. un., 27 marzo 2008, Fisia Italimpianti Spa e altri, in Mass. Uff., n.239924). In tale occasione, infatti, la Cassazione ha precisato che nella ricostruzione della nozione in esame non può farsi ricorso a parametri valutativi di tipo aziendalistico - quali ad esempio quelli del "profitto lordo" e del "profitto netto" -, non fosse altro per il fatto che nel linguaggio penalistico l'espressione in discorso ha assunto sempre un significato oggettivamente più ampio rispetto a quello economico o aziendalistico, non venendo mai inteso come espressione di una grandezza residuale o come reddito di esercizio, determinato attraverso il confronto tra componenti positive e negative del reddito.

Secondo la Cassazione dunque la nozione di profitto assume significati diversi in relazione ai differenti contesti normativi in cui è il termine è chiamato. Per cui, in presenza di reati colposi di evento, posto che la responsabilità del reato è attribuita all'ente in quanto la condotta violativa delle regole cautelari è stata assunta nel suo interesse, "l'idea di profitto si collega con naturalezza ad una situazione in cui l'ente trae da tale violazione un vantaggio che si concreta, tipicamente, nella mancata adozione di qualche oneroso accorgimento di natura cautelare, o nello svolgimento di una attività in una condizione che risulta economicamente favorevole, anche se meno sicura di quanto dovuto".

INFORMATICA FORENSE

di Marco Tullio Giordano, avvocato in Milano, e Giuseppe Dezzani, Digital Forensic Bureau, Torino

Le frodi man-in-the-middle, truffe informatico-finanziarie che provocano danni da migliaia di euro alle aziende grazie alla violazione della corrispondenza aziendale e ad un pizzico di social engineering.

Anche se l'ormai classico phishing, fattispecie criminosa riconducibile alla sostituzione di persona ed alla frode informatica, è divenuta largamente riconoscibile ed in parte evitabile dalla maggioranza degli utenti della rete, nuove e più pericolose varianti sembrano farsi strada tra i cybercriminali. E, proprio come per le infezioni nel mondo reale, pare che queste nuove varianti evolute siano più aggressive, più mirate, più resistenti e, soprattutto, più remunerative per i criminali ed estremamente dannose, sul piano finanziario, per le vittime. Oggi la nuova frontiera è il "man in the mail", versione riadattata in chiave informatica, di quel "man in the middle" (letteralmente l'uomo in mezzo) che fu usato come meccanismo del film "La stangata". Negli ultimi mesi, infatti, si sono intensificati gli episodi di truffe finanziarie online ai danni delle aziende di quasi tutta Europa, opera di criminali informatici ed organizzazioni transnazionali che sono riuscite a colpire anche molte società italiane.

L'attacco MITM (acronimo di man-in-the-middle), sostanzialmente, è un tipo di attacco silente nel quale l'agente si inserisce nei sistemi della vittima o del suo interlocutore (la dicitura man-in-the-middle si riferisce proprio alla posizione del portatore dell'attacco, interposta tra le due vittime) e per un lungo periodo di tempo, monitorandolo, ne studia le abitudini informatiche, leggendo e modificando, senza darne evidenza, le comunicazioni tra le due parti e nascondendo la sua presenza ad entrambe. Il meccanismo è molto semplice: gli "hacker" violano la casella email di una società, scelta con cura tramite valutazioni principalmente basate sul fatto che effettui operazioni internazionali di import/export, in modo da essere certi che essa abbia una relazione commerciale con un partner o con un fornitore estero. Per poter entrare nelle caselle di posta i criminali utilizzano metodi come phishing, brute forcing o persino trojan inviati via posta sui computer o sui

telefoni di chi, all'interno dell'azienda, gestisce i rapporti finanziari con l'estero. La posta elettronica viene poi monitorata per diverso tempo, in maniera da essere difficilmente individuabile, fino al momento in cui vengono scambiate i documenti utili all'importazione o esportazione di materiali, spesso con ingenti capitali in gioco. Al momento giusto i truffatori inviano un'email, fingendo di essere il fornitore estero (attraverso l'artificio della creazione di una casella di posta elettronica simile a quella originale) in cui chiedono che il pagamento per i beni acquistati o venduti avvenga su un differente istituto di credito, con tanto di specificazione delle coordinate bancarie di destinazione, spesso modificando graficamente il modulo d'ordine originale. Il messaggio appare solitamente autentico agli occhi dell'interlocutore, poco attento o non avvezzo allo strumento informatico, proprio per tutte le informazioni che i truffatori hanno potuto acquisire dall'email durante le settimane di monitoraggio. Per leggerezza o troppa fiducia, il cliente dall'altra parte esegue il bonifico utilizzando le nuove coordinate, in alcuni casi chiedendo conferma del cambio con una semplice email, alla quale i criminali rispondono fingendosi la controparte e tranquillizzando circa la legittimità del nuovo conto. I soldi vengono quindi bonificati su un conto in realtà intestato a dei prestanome (i c.d. "financial manager", già utilizzati indebitamente nei primi casi di phishing a cui siamo ormai stati abituati), dal quale poi entro pochi giorni spariscono senza possibilità di recupero.

Sotto il profilo del diritto penale, la fattispecie può essere inquadrata quale una vera e propria truffa ex art. 640 c.p. (la vittima è indotta in errore tramite artifizi e raggiri, consistenti nella falsa email a nome del fornitore e nell'uso di falsa documentazione contabile), piuttosto che scissa in molteplici condotte, avvinte dal vincolo della continuazione, riconducibili ai reati di sostituzione di persona ex art. 494 c.p. e di frode informatica ex art. 640 ter c.p., soprattutto a seguito della recente modifica legislativa introdotta dall'art. 9, comma 1, D.L. 14.08.2013, n. 93, così come modificato dall'allegato alla legge di conversione L. 15.10.2013, n. 119, che ha previsto l'inserimento di un comma specifico avente ad oggetto la commissione della frode mediante furto o utilizzo indebito dell'identità digitale altrui (letteralmente: "La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti"). Le circostanze che rendono, tuttavia, difficile se non addirittura impossibile incardinare l'azione penale nei confronti degli autori delle condotte illecite

sono relative ai limiti temporali (quando ci si accorge della truffa, solitamente i soldi sono stati sottratti dal conto di destinazione) e giurisdizionali (per nostra esperienza diretta, le connessioni risultano sempre originate da Paesi stranieri quali la Costa d'Avorio, la Russia o altri territori che non garantiscono l'assistenza giudiziaria necessaria per l'individuazione e la repressione dei colpevoli), che rendono la presentazione di denunce-querele contro ignoti più un adempimento burocratico che una effettiva soluzione del problema.

In aggiunta a ciò, anche sul parallelo versante civilistico della eventuale ripetizione dell'indebito pagamento mediante interpello della banca disponente e, soprattutto, di quella del beneficiario (sebbene sine titulo), l'unica strada percorribile sembrerebbe quella di richiedere lo storno del pagamento nel più breve tempo possibile. Una soluzione purtroppo esperibile solo fintantoché i fondi sono ancora presenti sul conto di destinazione. Del resto, ove – come nella maggioranza dei casi concretamente accade – la richiesta di ripetizione dell'indebito pagamento arrivi in ritardo e a conto ormai "svuotato", neppure sembrerebbe possibile addebitare alcuna responsabilità alle imprese creditizie: deve infatti essere sottolineato che le disposizioni comuni europee (discendenti tutte dalla direttiva 2007/64/CE del Parlamento europeo e del Consiglio, relativa ai servizi di pagamento nel mercato interno), declinate poi nei testi normativi quali il Payment Service Regulation (PSR) inglese del 2009 (specificamente l'art. 74, rubricato "Liability - Incorrect unique identifiers") o in Italia il Decreto Legislativo 27 gennaio 2010, n. 11 (specificamente all'art. 24, rubricato "Identificativi unici inesatti") tendono a giustificare – e di conseguenza a garantirne l'efficacia – le disposizioni di pagamento in cui l'indicazione del titolare del conto e le relative coordinate bancarie non coincidono, finendo di fatto per escludere ogni responsabilità in capo alle banche.

Di certo permane il dubbio circa l'adeguatezza di normative di tale portata, soprattutto in un'epoca in cui la semplicità e la velocità dei pagamenti online ha, di fatto, trasferito ogni possibilità di controllo nelle mani degli intermediari finanziari. Gli istituti di credito, del resto, sarebbero già dotati di strumenti di verifica e alert automatici che, con facilità, possano individuare operazioni potenzialmente sospette perché gravate da macroscopiche incongruenze (quale l'indicazione di un beneficiario diverso dal titolare del conto) o altri parametri sentinella, quali ad esempio l'atipicità della

disposizione, la transnazionalità o il coinvolgimento di utenti privati nel corso di operazioni commerciali. Il consiglio, in via residuale, non rimane che quello di una attenta prevenzione dei rischi di questo genere, con la previsione e l'attivazione di procedure interne di controllo e verifica delle informazioni, nonché di adeguamento della sicurezza informatica aziendale: in molti casi basterebbe la verifica dell'indirizzo del mittente, perché è piuttosto facile crearne uno molto simile a quello originale e soprattutto impostare il nome del mittente identico a quello corretto. In caso di pagamenti di importo elevato, poi, sarebbe preferibile porre in essere sempre un controllo con canali di comunicazione alternativi - una telefonata o un fax – per confermare esattamente richieste anomale ricevute via email.

Negli Stati Uniti l'FBI ha pubblicato da tempo un avviso utile alla prevenzione, diramato poi alle aziende potenzialmente aggredibili attraverso tale meccanismo. In attesa che il legislatore, o le associazioni di categoria, si attivino anche nel vecchio continente per porre un freno al fenomeno, l'unica soluzione quindi sembra essere quella della previsione di forti strumenti di prevenzione interni, poiché una volta che il pagamento è stato disposto, risultano davvero remote le possibilità di rientrare in possesso di quanto indebitamente trasferito su conti estranei a quelli sottesi al rapporto sinallagmatico con i propri fornitori.

Su questa tipologia di truffa non dobbiamo pensare solo in ottica di danno subito. La diffusione in rete di questa modalità di operare ha fatto si che alcune aziende abbiano pensato di simulare l'accesso alla propria email e fintamente cadere nell'inganno, facendo così trasferire fondi su un conto corrente estero ed inserendoli a perdita nel proprio bilancio. In realtà altro non era che la produzione di un fondo nero di valuta. Questo porta a segnalare anche agli organismi di vigilanza di prestare la massima attenzione, rientrando in questo caso in una diversa fattispecie di reato, rientrante proprio tra quelli previsti dal D.Lgs. 231/01. In questi casi un'attenta valutazione tecnica ha permesso di capire che la truffa era stata simulata e non subita, e che l'azienda aveva architettato una specifica condotta per trasferire una quantità importante di fondi su un conto corrente estero, pensando poi di poterne disporre successivamente, una volta che la querela depositata in Procura sarebbe stata archiviata, come spesso accade in questi casi.

NORME E ATTI

di Andrea Ferrero, Redazione Rivista 231

Attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici

L'Autorità Nazionale Anticorruzione ha definitivamente approvato, con la Determinazione n. 8 del 17 giugno 2015, le "Linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici" poste in consultazione pubblica dal 25 marzo al 15 aprile 2015.

Le Linee guida sono volte a orientare tutte le società e gli enti di diritto privato in controllo pubblico o a partecipazione pubblica non di controllo, nonché gli enti pubblici economici nell'applicazione della normativa in materia di prevenzione della corruzione, di cui alla legge 6 novembre 2012, n. 190, e trasparenza, di cui al decreto legislativo 14 marzo 2013, n. 33, con l'obiettivo primario che essa non dia luogo a un mero adempimento burocratico, quanto invece venga adattata alla realtà organizzativa delle singole società e enti per mettere a punto strumenti di prevenzione mirati e incisivi.

Le Linee guida si rivolgono anche alle amministrazioni controllanti, partecipanti e vigilanti cui spetta attivarsi per assicurare o promuovere, in relazione al tipo di controllo o partecipazione, l'adozione delle misure di prevenzione e trasparenza. .
I contenuti delle Linee guida costituiscono il risultato dei lavori svolti dal Tavolo congiunto istituito dall'Autorità nazionale anticorruzione e dal Ministero dell'Economia e delle Finanze (MEF).
Esse non riguardano le società con azioni quotate e quelle emittenti strumenti finanziari quotati in mercati regolamentati per le quali l'Autorità adotterà, entro il mese di luglio 2015, specifiche Linee guida.

PRIVACY

di Patrizia Ghini, dottore commercialista e pubblicista in Milano

Controlli a distanza dei lavoratori

A seguito delle modifiche apportate ai sensi del Jobs Act allo Statuto dei lavoratori, in materia di controlli a distanza, è nato un acceso dibattito, di cui danno notizia diffusamente anche i mass media.
La Legge 10 dicembre 2014, n. 183 (GU n. 290 del 15/12/2014) ha conferito delega al Governo in materia di riordino, tra l'altro, della disciplina dei rapporti di lavoro.
La legge delega (cd. "Jobs act"), all'art. 1, co. 7, lettera f), stabilisce che il Governo adotti – entro sei mesi dalla data di entrata in vigore della medesima legge – decreti legislativi attuativi specifici a completamento delle modifiche in alcuni degli ambiti toccati dalla legge delega.
Uno di essi, quindi, avrebbe dovuto contenere un testo organico (semplificato) delle discipline delle tipologie contrattuali e dei rapporti di lavoro, nel rispetto dei princìpi e criteri direttivi ivi specificati, in coerenza on la regolamentazione della UE e delle convenzioni internazionali, ed in particolare quello di "revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore".
Nella seduta del 12 giugno, il Governo ha approvato e inviato alle Camere, per il previsto parere (non vincolante), la bozza del decreto legislativo attuativo della delega sulle semplificazioni che, tra l'altro, prevede all'art. 23 una proposta di modifica all'articolo 4 della legge 20 maggio 1970, n. 300 meglio noto come Statuto dei Lavoratori.
L'orientamento altalenante e controverso della Giurisprudenza evidenzia da molti anni la necessità di un intervento legislativo innovatore sull'art. 4, che introduca regole più chiare e recepisca sia alcune "massime" giurisprudenziali sia l'evoluzione tecnologica dei mezzi di controllo (l'art. 4 è stato redatto in un'epoca addirittura antecedente alla diffusione delle videocamere).

Il tema della legittimità dei controlli ha assunto una rilevanza ancora maggiore con l'introduzione, nel nostro ordinamento giuridico, dal 1995 in avanti, delle disposizioni in materia di tutela dei dati personali (attualmente,

d.lgs. 30/6/2003, n. 196). Il confine tra legittime esigenze del datore di lavoro e tutela della privacy del lavoratore è anch'esso di difficile definizione.
In passato, il Garante privacy è intervenuto stabilendo ad esempio che, per l'esercizio del suo potere di controllo, il datore di lavoro non può utilizzare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", tra cui rientrano anche "strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica", in quanto lesive della libertà e della dignità del lavoratore.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa e anche quando i singoli lavoratori ne siano consapevoli.(...)

Nell'incerto quadro interpretativo che riguarda il delicato tema dei controlli a distanza, si inserisce il recente Decreto Legislativo, approvato dal Governo il 12 giugno 2015 e attualmente in discussione presso alle Camere, il quale, all'art. 23 ("*Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196") stabilisce quanto segue:*
"1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente:
«ART. 4. Impianti audiovisivi e altri strumenti di controllo.
Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali. 2. La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai

sensi del primo e del secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196»

2. L'articolo 171 del decreto legislativo 30 giugno 2003, n. 196, è sostituito dal seguente:
«*ART. 171. Altre fattispecie.* La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970.»ART. 24 *(Cessione dei riposi e delle ferie).* Fermo restando quanto disposto dal decreto legislativo 8 aprile 2003, n. 66, i lavoratori possono cedere a titolo gratuito ".
La (proposta di) riforma, relativamente ai sistemi audiovisivi, con particolare riguardo alla loro riconducibilità o meno all'obbligo di accordo sindacale, prevede innovativamente che:
1. gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati anche per la sicurezza del lavoro e per la tutela del patrimonio aziendale (oltre che per le già previste esigenze produttive e organizzative);
2. non è tuttavia necessario l'accordo con le rappresentanze sindacali in caso di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze": è questo passaggio della proposta di riforma che crea maggiori contestazioni.
3. "le informazioni raccolte dal datore di lavoro a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196": occorre quindi rispettare, per poter utilizzare legittimamente le evidenze raccolte tramite i sistemi di controllo, l'obbligo informativo di cui all'art. 13 del D.Lgs. 196/2003 nonché quanto previsto dalle direttive del Garante privacy. Resta perciò da applicare in modo completo la normativa in materia di protezione dei dati personali, che comunque pone vincoli non irrilevanti al potere datoriale di porre in essere attività di raccolta di dati personali tramite sistemi di controllo.

Le novità in materia di controlli a distanza sono state spiegate tramite la Relazione illustrativa di accompagnamento del provvedimento sulla

emplificazione delle procedure e degli adempimento a carico di cittadini e imprese. Il Governo indica che, in sostanza, non avranno bisogno di alcun via libera formale i controlli effettuati sugli strumenti utilizzati dal lavoratore per rendere operativa la prestazione lavorativa e su quelli di registrazione degli accessi e delle presenze. I dati che emergeranno da tali controlli potranno essere "utilizzati ad ogni fine connesso al rapporto di lavoro, purché sia data al lavoratore adeguata informazione circa le modalità d'uso degli strumenti e l'effettuazione dei controlli, sempre, comunque, nel rispetto del Codice privacy".

E' evidente, tuttavia, che le spiegazioni del Governo non hanno risolto tutti i dubbi. Resterebbe la caratteristica di divieto "flessibile", la cui applicabilità, tuttavia, sembrerebbe più ampia.
Sulle novità in analisi è intervenuto anche il Garante per la privacy, che ha osservato come "Un più profondo monitoraggio di impianti e strumenti non deve tradursi in una indebita profilazione delle persone che lavorano", auspicando che "il decreto legislativo all'esame delle Camere sappia ordinare i cambiamenti resi possibili dalle innovazioni in una cornice di garanzie che impediscano forme ingiustificate e invasive di controllo, nel rispetto della delega e dei vincoli della legislazione europea".
L'attività di vigilanza espletata dall'Odv può comportare l'utilizzo di evidenze raccolte con sistemi di controlli a distanza attuati dalla società. Ne deriva, pertanto, la rilevanza della problematica anche nell'ambito dei modelli organizzativi.

PROFILI INTERNAZIONALI

di Giovanni Tartaglia Polcini, Magistrato, Consigliere giuridico presso il Ministero degli Affari Esteri e Paola Porcelli, Avvocato, patrocinante in Cassazione, Foro di Benevento

La responsabilità degli enti derivante da reato, ancora al centro del dibattito nei fora multilaterali anticorruzione.

La responsabilità degli enti derivante da reato, nel nostro ordinamento disciplinata dal decreto legislativo 231 del 2001, come successivamente modificato e integrato, costituisce centro permanente di interesse e discussione a livello internazionale e multilaterale.
Il dibattito è particolarmente intenso allorquando si discute delle misure da adottare per prevenire e contrastare la corruzione, soprattutto nelle transazioni internazionali.
Sia in sede WGB OCSE, sia in sede di working group anticorruzione del G20, così come nel gruppo GRECO, e ancora in sede di verifica dell'applicazione della convenzione delle Nazioni Unite per il contrasto alla corruzione, si confrontano le diverse risposte ordinamentali alla necessità di prevedere, oltre alla responsabilità delle persone fisiche, per una serie di reati, anche la responsabilità degli enti, in sede di procedimento penale e di diritto sostanziale criminale.

Segnatamente, l'OCSE non esita a emettere vere e proprie raccomandazioni per gli Stati aderenti alla convenzione, aventi ad oggetto la necessità di rinforzare le previsioni ordinamentali in materia di responsabilità degli enti derivante da reato.
Anche l'Italia, così come la Spagna, sono state in passato raggiunte da specifiche raccomandazioni, per il rafforzamento della responsabilità degli enti derivante da reato, alle quali hanno ottemperato con particolare precisione e puntualità.
Già abbiamo avuto modo di sottolineare come proprio il D.Lgs. 231 del 2001 risponda all'esigenza di “dialogo” fra le grandi imprese e la pubblica amministrazione nazionale, a fini di penetrazione della cultura della legalità "dal basso", così che l'attività di impresa non perda la propria autonoma dimensione etica, anche a fini di rafforzamento della fiducia dei consumatori nell'attività economica privata.

La 231 risponde anche all'esigenza di avviare un "trialogo" costruttivo (fra Governo, impresa e società civile) nella trasparenza del coinvolgimento del settore pubblico e di quello privato, congiuntamente, al fine di contrastare fenomeni di devianza e soprattutto la corruzione.
In quest'ottica, particolare attenzione riveste la questione della necessità di applicare il sistema di responsabilità degli enti anche alle imprese pubbliche, intendendosi per tali le imprese di proprietà totale o parziale dello Stato o di altro ente pubblico.
Le cosiddette public ownership enterprises sono difatti i soggetti maggiormente coinvolti, nella casistica globale, in fatti di corruzione internazionale, aventi ad oggetto appalti di opere pubbliche e di pubbliche forniture. Ed è proprio con riferimento a simile questione che si pongono le problematiche più importanti in tema di responsabilità degli enti a livello internazionale.

Da un lato, invero, ci si imbatte talvolta in limiti di carattere normativo che, tenuto conto della natura giuridica di suddetti enti, impediscono a livello legislativo di investigare e di punire condotte corruttive. Dall'altro, ad onor del vero, anche quando ci si trova di fronte alla possibilità in astratto di investigare e punire, normativamente prevista, le difficoltà provengono dalla prassi operativa, per le ragioni di seguito specificate.
Ed invero, laddove non esiste una piena autonomia ed indipendenza della magistratura dal potere esecutivo, e lo stesso potere esecutivo controlla e vigila sugli enti pubblici, ivi comprese le imprese, appare seriamente difficile che possa avviarsi un'attività di investigazione, per una genuina presa di coscienza dell'esistenza di fenomeni corruttivi a livello di appalti internazionali.

Tanto spiega il crescente interesse che, in sede multilaterale, si presta al nostro ordinamento che assurge, sempre più, a modello.
L'Italia, difatti, sempre più viene coinvolta in attività di Capacity building e di law enforcement in materia di lotta alla corruzione, soprattutto in materia di responsabilità degli enti derivante da reato e di misure proattive di coinvolgimento della società civile nel controllo di legalità. A diversa conclusione, invece, deve giungersi nel nostro ordinamento: l'indipendenza e l'autogoverno della magistratura inquirente e requirente, così come di quella giudicante, assicurano difatti una terzietà dell'organo deputato all'investigazione e all'indagine.

Suddetta specificità, propria dell'Italia, è destinata, unitamente ad altre caratteristiche di recente emersione nel nostro ordinamento, a giocare un ruolo fondamentale nell'aumento dell'affidabilità e del rating dell'Italia sul piano anticorruzione a livello globale. .

Ciò posto, si comprende anche l'espansione del sistema 231 in corso nel nostro Paese, la proliferazione delle figure di reato presupposto della responsabilità degli enti e la torsione del meccanismo di prevenzione, da modello di disciplina dell'impresa illecita, a ordine economico legalmente orientato, nell'ambito di un complessivo disegno riformatore della giustizia e dell'economia, volto a promuovere la crescita e l'occupazione oltre che ad attrarre gli investimenti esteri. .

Sta per avviarsi proprio in questo periodo la quarta fase di revisione e di self assessment dei paesi aderenti alla convenzione OCSE.
Uno dei capitoli più importanti della verifica, senza dubbio, avrà proprio ad oggetto l'applicazione delle regole condivise in materia di responsabilità degli enti derivante da reato. In questo settore, indubitabilmente, l'Italia e' ben al di là della media mondiale e può costituire termine di riferimento assoluto.

SOCIETÀ ED ENTI PUBBLICI

di Carlo Manacorda, Docente di Pianificazione, programmazione e controllo delle aziende pubbliche, Università degli Studi di Torino

L'A.N.AC. adotta, definitivamente, le linee per la tutela del whistleblower. Le direttive per gli enti di diritto privato in controllo pubblico, pubblici economici e di diritto privato partecipati da pubbliche amministrazioni

L'Autorità Nazionale Anticorruzione (A.N.AC.) ha definitivamente approvato, con determina n. 6 del 28 aprile 2015 (G.U. n. 110 del 14.05.2015), le "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)". Il provvedimento era stato posto in consultazione pubblica dal 24 febbraio al 16 marzo 2015.
Questa Circolare aveva già dedicato all'argomento qualche annotazioni nel n. 3 – marzo 2015. Alcune direttive contenute nella stesura definitiva delle Linee guida rivolte a particolari categorie di enti pubblici suggeriscono, tuttavia, di ritornare ancora brevemente sul tema. Questo poiché le Linee guida, nella versione ultima, rinviano ad altre direttive frattanto emanate dalla stessa A.N.AC. – congiuntamente al Ministero dell'economia e delle finanze (MEF) – in materia di prevenzione della corruzione da parte di alcuni soggetti pubblici. Il rinvio è alle "Linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e della trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici", poste in consultazione pubblica fino al 15 aprile 2015.

Anche nella redazione finale, le Linee guida ridelineano il quadro normativo che ha introdotto, nell'ordinamento italiano, la fattispecie del dipendente pubblico che "denuncia all'Autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico, condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro" (art. 1, c. 51, l. 190/2012, che aggiunge l'art. 54-bis nel D.Lgs. 165/2001). Sulla base delle norme vigenti, obiettivo generale delle Linee guida è quello di "dettare una disciplina volta a incoraggiare i dipendenti pubblici a denunciare gli illeciti e, al contempo, a garantirne un'efficace tutela". Si ribadisce che, per dipendente pubblico, non s'intende soltanto chi ha un rapporto d'impiego con la Pubblica Amministrazione, ma anche coloro che svolgono attività all'interno di uffici

pubblici (collaboratori, consulenti, titolari di organi e di incarichi ed anche collaboratori di imprese fornitrici delle stesse amministrazioni). Si precisa però che le Linee guida in materia di tutela del whistleblower non possono andare oltre a quanto stabilito dall'articolo 54-bis del D.Lgs. 165/2001. Conseguentemente, non disciplinano le modalità di trattazione di altre tipologie di segnalazione quali quelle provenienti da cittadini o imprese, ovvero le segnalazioni anonime (queste ultime peraltro considerate se adeguatamente circostanziate e tali da far emergere fatti e situazioni relazionandoli a contesti determinati). Tuttavia l'A.N.AC., ricordando che l'articolo 31 del decreto-legge 90/2014, convertito nella legge 114/2014 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza negli uffici giudiziari) l'ha inserita tra i soggetti che, con l'Autorità giudiziaria e la Corte dei conti, possono ricevere le denunce di illeciti, osserva che queste, ove non pervengano da dipendenti pubblici nel senso prima precisato, avranno trattamenti diversi da quelli specificamente previsti dall'articolo 54-bis per la tutela del dipendente pubblico.

Resta confermato l'ampio concetto di "condotte illecite" oggetto delle segnalazioni. Vi rientra l'intera gamma dei delitti contro la Pubblica Amministrazione. Ma vi rientrano anche i comportamenti di chi abusi del potere affidatogli per ottenere vantaggi privati, indipendentemente dalla rilevanza penale dei fatti (sprechi, nepotismo, assunzioni non trasparenti, irregolarità contabili, violazione delle norme ambientali e di sicurezza sul lavoro, ecc.). La prima tutela assicurata al denunciante è la riservatezza sulla sua identità. Inoltre, è tutelato ove avessero ad adottarsi, nei suoi confronti, "misure discriminatorie, dirette o indirette, aventi effetti sulle condizioni di lavoro per motivi collegati, direttamente o indirettamente, alla denuncia". Denuncia però che non deve sfociare in casi di responsabilità per calunnia o diffamazione, o comportare un risarcimento per danni. Se venissero accertate in sede giudiziale responsabilità di questa natura, cessa le tutela a favore del denunciante. Sul punto l'Autorità conclude che, pur essendo consapevole delle lacune normative per queste ipotesi, "ritiene che solo in presenza di una sentenza di primo grado sfavorevole al segnalante cessino le condizioni di tutela dello stesso". Complicazioni di questo genere non sembra possano incentivare soggetti a denunciare le malefatte nei confronti dell'amministrazione. Il rischio di una sentenza sfavorevole al denunciante è sempre presente. In questo caso, il denunciante finirebbe davvero nei guai.

Come detto prima, le Linee guida recano alcune direttive riguardanti particolari categorie di enti pubblici. Una Parte (IV) è dedicata alla "Tutela del dipendente che segnala condotte illecite negli enti di diritto privato in controllo pubblico e negli enti pubblici economici". L'Autorità afferma, preliminarmente, di ritenere che l'applicazione delle disposizioni in materia di prevenzione della corruzione di cui alla legge 190/2012 sia da estendere anche agli enti di diritto privato in controllo pubblico di livello nazionale e locale nonché agli enti pubblici economici. Muovendo da questa considerazione, rinvia alle altre "Linee guida" richiamate in precedenza dove ha stabilito regole sul tema anche per questi enti. Lì ha puntualizzato.

- Enti di diritto privato in controllo pubblico. Si tratta di un quadro di soggetti particolarmente complesso. Vi appartengono, soprattutto, "fondazioni" e "associazioni" che hanno natura privatistica, che non necessariamente hanno personalità giuridica, ma che nei confronti delle quali sono riconosciuti, in capo alle amministrazioni pubbliche, poteri di controllo, deducibili da particolari indicatori[1]. Questi enti sono tenuti all'applicazione della normativa sulla prevenzione della corruzione ai sensi dell'articolo 1, comma 60, della legge 190, dell'articolo 11 del D.Lgs. 33/2013 e dell'articolo 1, comma 2, del D.Lgs. 39/2013. Ciò comporta che devono adottare il Piano di prevenzione della corruzione e nominare il Responsabile della prevenzione della corruzione. Se hanno già adottato il Modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001, devono integrarlo con disposizioni idonee a prevenire anche i fenomeni di corruzione in coerenza con le finalità della legge 190/2012.
- Enti pubblici economici. Previsti dall'articolo 2201 e ss. del codice civile, perseguono finalità pubbliche attraverso l'esercizio di attività d'impresa. In materia di lotta alla corruzione, sono tenuti all'applicazione delle norme della legge 190/2012 nei termini previsti per le società in controllo pubblico (individuate ex art. 2359, c. 1, nn. 1 e 2 cod. civ.) poiché, diversamente, si creerebbe una ingiustificata asimmetria con queste. Quanto alle modalità di applicazione della legge 190/2012, devono

[1] Si indicano, in via esemplificativa: 1) l'istituzione dell'ente in base alla legge o atto amministrativo dell'amministrazione interessata, oppure la predeterminazione, ad opera della legge, delle finalità istituzionali; 2) la nomina dei componenti degli organi di indirizzo e/o direttivi e/o di controllo da parte dell'amministrazione; 3) il prevalente o parziale finanziamento dell'attività istituzionale con fondi pubblici o il riconoscimento agli enti del diritto di percepire contributi pubblici . Da ciò deriva che la gestione finanziaria degli stessi sia soggetta al controllo della Corte dei conti; 4) il riconoscimento di poteri di vigilanza per l'approvazione dello statuto, delle delibere più significative in materia economico finanziaria, ecc.; 5) la limitazione dell'apporto di capitale privato; 6) per le associazioni, la titolarità pubblica della maggioranza delle quote.

comportarsi in maniera analoga a quanto detto sopra per gli enti di diritto privato in controllo pubblico.

Guardando alla gestione dell'istituto del whistleblower, l'Autorità suggerisce che le amministrazioni controllanti e vigilanti promuovano, da parte dei suddetti enti, l'inserimento nei Piani di prevenzione della corruzione – ovvero nel Modello del D.Lgs. 231/2001 integrato con la legge 190/2012 – di misure analoghe a quelle previste dalle Linee per i dipendenti pubblici. Suggerisce analoghe iniziative anche per le società e gli enti di diritto privato partecipati da pubbliche amministrazioni, soggetti cioè che svolgono anche attività di pubblico interesse beneficiando di risorse pubbliche, ma limitatamente a queste attività. L'Autorità auspica comunque un intervento del legislatore per colmare il vuoto normativo esistente in materia di dipendenti di questi enti che segnalino illeciti nei termini previsti dall'articolo 54-bis del D.Lgs. 165/2001.