Circolare 231

approfondimenti, notizie e informazioni

n. 10 – novembre 2015

PLENUM

rivista231.it

Sommario

AMBIENTE E SICUREZZA

di Marina Zalin, Butti & Partners, Verona

La natura dell'illecito e il sequestro per equivalente

Con sentenza del 30 settembre 2015 (c.c. 14 aprile 2015) n. 39373 la Corte di Cassazione esamina un'ordinanza cautelare reale con la quale il giudice del riesame aveva annullato un provvedimento di sequestro per equivalente, disposto nei confronti di una società alla quale erano stati contestati gli illeciti amministrativi da reato connessi alla contravvenzione di cui all'art. 256 d.lgs. 152/2006 ed al delitto di attività organizzata per il traffico illecito di rifiuti.
Il Tribunale aveva escluso l'applicabilità di tale misura tenuto conto che i reati ambientali ipotizzati a carico degli indagati sarebbero stati consumati prima dell'entrata in vigore della norma con la quale sono state introdotte, tra i reati presupposto della responsabilità amministrativa degli enti, le fattispecie previste dall'art. 256 e dall'art. 260 d.lgs. 152/2006.
La Procura proponeva, avverso tale pronuncia, ricorso per Cassazione sostenendone l'erroneità stante la natura permanente dei reati, il mancato accertamento del ripristino dei luoghi entro l'entrata in vigore del d.lgs. 121/2001 e, pertanto, la non intervenuta consumazione degli stessi prima di tale momento.

La Cassazione, in parziale accoglimento dell'impugnazione proposta così argomenta:
- il reato di abbandono di rifiuti e di discarica abusiva sono reati eventualmente permanenti. Gli stessi si consumerebbero, quindi, in alternativa al momento del rispristino dello stesso dei luoghi, al momento della sottrazione della disponibilità del bene mediante misura cautelare reale od al momento della pronuncia della sentenza di primo grado;
- il reato di attività organizzata per il traffico illecito di rifiuti è, invece, reato abituale la cui consumazione quindi giunge al momento di realizzazione dell'ultimo atto posto in essere dagli indagati;
- con riferimento a tali fattispecie viene ritenuta corretta, quantomeno nelle sue conclusioni, l'ordinanza adottata dal tribunale del riesame che, in assenza di indizi di prosecuzione dell'attività di gestione dei rifiuti successivamente alla data di introduzione dei reati ambientali nel d.lgs. 231/2001, non ha ritenuto adottabile il decreto di sequestro per equivalente.

Tale conclusione, osserva la Corte, è rispettosa del principio di legalità ribadito dal legislatore anche in tale materia.
A differente conclusione giunge, invece, la Corte con riferimento alle altre ipotesi di reato poste a fondamento della misura adottata.
La Suprema Corte riconduce, infatti, il reato di stoccaggio di rifiuti alla categoria del reato permanente, che si consumerebbe solo allorché la situazione di illiceità sia stata eliminata; tali conclusioni non possono essere condivise.

Nell'ipotesi di illecita condotta consistente nello smaltimento di rifiuti la contravvenzione ha natura istantanea, come affermato dalla Cassazione (Cass. 13 aprile 2010, n. 22034 secondo la quale "la contravvenzione di attività di smaltimento di rifiuti in mancanza della prescritta autorizzazione, di cui all'art. 256 comma 1 d.lgs. n. 152 del 2006, ha natura di reato istantaneo che si perfeziona nel momento in cui si realizza la singola condotta tipica."). Alla stessa disciplina deve essere ricondotto lo stoccaggio che è infatti definito, in senso tecnico, come attività di smaltimento consistente nelle operazioni di deposito preliminare di rifiuti di cui al punto D15.
Peraltro, anche in relazione al reato di abbandono e deposito incontrollato di rifiuti, che apparentemente potrebbe generare maggiori dubbi, la Cassazione ne ha escluso la natura di reato permanente. Se l'abbandono è funzionale ad un uno smaltimento ulteriore il reato "dura" sino allo smaltimento, mentre qualora non sia prevista alcuna successiva attività di movimentazione del rifiuto é al momento dell'abbandono che il reato deve considerarsi consumato.

Quanto al reato di omessa bonifica, la Suprema Corte – rifacendosi ad un orientamento pregresso, che si ritiene tuttavia poco convincente, quanto meno nella sue spesso esasperate conseguenze, - lo ritiene perdurante sino al completamento della bonifica dell'area non essendo idoneo neppure l'intervenuto sequestro ad individuare il termine ultimo di consumazione dell'illecito. Sostiene, infatti, la Corte che la misura ablatoria, in esecuzione della quale l'imputato è privato della disponibilità dell'area non sia sufficiente a far cessare la permanenza del reato.
L'argomentazione a sostegno di tale tesi è la seguente: il reato di omessa bonifica è omissivo permanente e l'antigiuridicità cessa con unicamente

azioni ripristinatorie al cui compimento non è di ostacolo l'ablazione del bene (Cass. 6098/2007).
Eppure, come evidenziato dalla sentenza Rubegni con riferimento al reato di discarica abusiva, il sequestro dell'area impedisce all'imputato di compiere sulla stessa ulteriori attività pur potendo chiederne la restituzione a tale unico fine; richiesta di restituzione che potrebbe, peraltro, essere rigettata dall'autorità giudiziaria, impedendo così all'imputato di procedere agli adempimenti previsti dalla legge. Non si comprende, quindi, in quale modo la natura del reato (omissivo permanente) possa incidere sulla idoneità o meno del sequestro di determinare la cessazione della permanenza. Anzi a contrario proprio la natura omissiva della fattispecie, atteso come sia necessario avere la disponibilità dell'area per procedere ai sensi dell'art. 242, impone che a sequestro intervenuto la consumazione sia considerata cessata.

ANTIRICICLAGGIO E ANTICORRUZIONE

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

Nuovo obbligo di autovalutazione per le banche

Nuovo obbligo in capo alle banche, che dovranno svolgere un'autovalutazione dei rischi di riciclaggio e di finanziamento del terrorismo. Si tratta di un *risk assessment* che dovrà essere periodicamente aggiornato.
Banca d'Italia, con nota del 21 ottobre 2015, ha chiesto infatti agli intermediari finanziari di adeguarsi a quanto già dettato a livello comunitario, mettendo in essere un processo articolato in più fasi. Si tratta di un'attività nuova e mai svolta sino ad oggi dalle banche italiane. Nella nuova impostazione vengono introdotti tre livelli di valutazione del rischio: comunitario, nazionale e intermediario.

A livello comunitario la Commissione Europea dovrà effettuare una valutazione dei rischi che gravano sul mercato interno e relativi alle attività transfrontaliere. In tal senso, la Commissione elaborerà una relazione che identifica, analizza e valuta i rischi a livello europeo.
In relazione al secondo livello, ciascuno Stato è tenuto ad adottare idonee misure per individuare, valutare, comprendere e mitigare i rischi di riciclaggio che lo riguardano. Valutazione che dovrà essere tempestivamente messa a disposizione degli intermediari per facilitare l'esecuzione del loro *risk assessment*.

Infine, gli intermediari saranno tenuti a individuare e valutare i rischi di riciclaggio in considerazione dei clienti con cui operano, dei paesi o aree geografiche di attività, dei prodotti o servizi offerti, e dei canali e delle modalità di distribuzione.

La metodologia indicata dall'Autorità di Vigilanza prevede lo svolgimento di varie fasi di lavoro.
La prima, consiste nell'identificazione dei rischi attuali e potenziali cui l'intermediario è o può essere esposto in base alla natura e all'estensione dell'attività svolta, in considerazione anche di fonti esterne, fra cui l'analisi nazionale del Comitato di Sicurezza Finanziaria.

La seconda fase di lavoro riguarda l'analisi dell'adeguatezza dell'assetto organizzativo e dei presidi aziendali rispetto ai rischi precedentemente identificati al fine di individuare eventuali vulnerabilità. In ultimo, la determinazione del rischio residuo cui è esposto l'intermediario e relative modalità di mitigazione.

GIURISPRUDENZA ANNOTATA

di Ciro Santoriello, Sostituto Procuratore presso il Tribunale di Torino

Responsabilità degli enti per il delitto di associazione a delinquere transnazionale

La decisione

Reati presupposto della responsabilità degli enti – Associazione a delinquere transnazionale – Rinvenimento di un profitto derivante direttamente dal delitto di associazione a delinquere a prescindere dal profitto derivante dalla commissione dei singoli reati scopo – Sussistenza – Sequestro preventivo del profitto derivante dal reato associativo – Ammissibilità (C.p., art. 416; C.p.p., art. 321; legge n. 146 del 2006, artt. 3 e 4; d.lgs. n. 231 del 2001, artt. 2, 19, 53)

Con riferimento alla responsabilità degli enti per reati associativi transnazionali, il profitto derivante dalla commissione di tali illeciti – da sottoporre ad eventuale sequestro preventivo e successiva confisca - può consistere anche nel complesso dei vantaggi direttamente conseguenti dall'insieme dei reati fine, dai quali il reato associativo è del tutto autonomo e la cui esecuzione è agevolata proprio dall'esistenza di una stabile struttura organizzativa e da un comune progetto delinquenziale (1).

CASSAZIONE PENALE – SEZIONE TERZA – C.C. 14 OTTOBRE 2015, N. 46162 (DEP. 23 NOVEMBRE 2015), SQUASSONI, PRESIDENTE – AMORESANO, RELATORE – SALZANO, P.M. (CONF.) – VERBATIM ITALIA S.P.A.

(1) 1. Come è noto, fra i reati presupposto della responsabilità degli enti rientra anche il delitto di associazione a delinquere. Questa previsione pone però un problema attinente l'ambito di applicazione del decreto legislativo n. 231 del 2001: infatti, posto che, come è noto, il novero dei reati presupposto della responsabilità delle società è tassativamente determinato dal legislatore, ci si domanda se le prescrizioni di cui al d.lgs. n. 231 debbano trovare applicazione anche laddove agli amministratori o dipendenti della società sia contestato il reato di associazione a delinquere

– di cui all'art. 24-ter d.lgs. n. 231 del 2001 – siano finalizzati alla commissione di delitti che, a loro volta, non rientrino fra gli illeciti presupposto della responsabilità della persona giuridica.
Per esemplificare, richiamando un'ipotesi assolutamente frequente, si pensi ad un'associazione a delinquere finalizzata – per il tramite di una pluralità di condotte di false fatturazione, parte delle quali tenute all'estero – all'evasione fiscale.
In proposito la dottrina si è espressa in termini positivi (TRAVERSI, Responsabilità amministrativa delle società anche per reati tributari?, in Resp. Amm. Soc. Enti, 2008, 3, 133), con particolare riferimento alle cosiddette "frodi carosello", espressione con cui si indicano condotte criminose poste in essere da più persone che - oltre a realizzare le fattispecie di cui agli artt.2 ed 8 d.lgs. n. 74 del 2000 – pongono in essere una associazione a delinquere rilevante ai sensi dell'art. 416 c.p. e che può assumere le caratteristiche del cosiddetto "reato transnazionale" di cui all'art. 3 della legge .n. 146 del 2006. Secondo gli autori sovra menzionati, posto che tra i reati transnazionali che, a norma dell'art. 10 della legge 146/2006, danno luogo a responsabilità amministrativa degli enti, vi è anche il delitto di "associazione per delinquere" di cui all'art. 416 c.p., nel caso in cui sia contestato il reato associativo a carattere transnazionale, finalizzato alla commissione di delitti di emissione e/o utilizzazione di fatture relative ad operazioni inesistenti, secondo lo schema delle frodi carosello, non c'è dubbio che, "accanto alla responsabilità penale delle persone fisiche che hanno commesso i reati di cui trattasi, vi sarà anche, a carico delle società appartenenti al sodalizio criminoso, una responsabilità amministrativa".

2. Sullo specifico punto ora esaminato, la Cassazione non fornisce un risposta esplicita, anche se la stessa può ricavarsi in via interpretativa ed indiretta dalla soluzione che la Corte ha fornito all'altro tema sottoposto alla sua attenzione ovvero la sussistenza di uno specifico profitto ricollegabile alla associazione a delinquere a prescindere dal provento derivante dalla commissione dei cosiddetti illeciti-fine – ovvero i reati alla cui commissione è diretta la costituita associazione.
Sul punto la Cassazione ribadisce un orientamento ormai consolidatosi, affermando che il delitto di associazione a delinquere può essere considerato in sé idoneo a generare un profitto, sequestrabile ai fini della successiva confisca (nello stesso senso Cass., sez. III, 27 gennaio 2011,

n.5869; Cass., sez. III, 24 febbraio 2011, n. 11969; Cass., sez. II, 26 giugno 2014, n. 28960).
Sulla base di tale affermazione può trarsi la conclusione che secondo la Cassazione la responsabilità dell'ente sussiste ogni qualvolta questi sia coinvolto in un'associazione a delinquere, a prescindere dal fatto che i reati scopo alla cui commissione l'associazione è diretta rientrino o meno nel novero degli illeciti presupposto della responsabilità dell'ente. Infatti, una volta che la Cassazione ha ammesso la possibilità di sottoporre a confisca il profitto che una società ha tratto dalla realizzazione di un'associazione criminosa cui hanno partecipato i suoi organi apicali – anche se tale associazione era diretta alla commissione di illeciti tributari e quindi non considerati dagli artt. 24 e seguenti d.lgs. n. 231 del 2001 – è evidente che a tale affermazioni si arrivi perché, per l'appunto, si ammette che la responsabilità dell'ente sussiste per il solo fatto di essere stato commesso il reato di cui all'art. 416 c.p..

Reati tributari e confisca del profitto in capo all'ente collettivo

La decisione

Reati tributari – Confisca e sequestro per equivalente – Reato commesso dall'amministratore o rappresentante legale di una persona giuridica in relazione ad obblighi tributari gravanti sulla medesima – Ammissibilità dell'adozione di un provvedimento cautelare reale sui beni della società – Condizioni (d.lgs 10 marzo 2000 n. 74, articolo 10; legge n. 244 del 2007, art. 143, comma 1; cod. pen., art. 322-ter)

In caso di commissione di un reato tributario da parte di amministratori o legali rappresentati di società ed enti, è possibile procedere nei confronti della persona giuridica al sequestro preventivo finalizzato alla confisca di denaro o di altri beni fungibili o di beni direttamente riconducibili al profitto di reato tributario in due sole ipotesi, ovvero 1) se la società o l'ente ha effettivamente maturato tale profitto a seguito del reato; 2) se la persona giuridica è solo uno schermo fittizio (1).

CASSAZIONE PENALE – SEZIONE SECONDA – C.C. 27 OTTOBRE 2015, N. 45520 (DEP. 16 NOVEMBRE 2015), ESPOSITO, PRESIDENTE – ALMA, RELATORE – GIALANELLA, P.M. (CONF..) – TERLIZZI.

(1) 1. La decisione ribadisce quanto asserito dalle Sezioni Unite 30 gennaio 2014, Gubert, su cui si vedano SANTORIELLO, Confiscabilità "limitata" dei beni della società per i reati commessi dall'amministratore, in Fisco, 2014, 13, 1255; CORSO, Reato non presupposto di responsabilità amministrativa e limiti del sequestro/confisca nei confronti dell'ente, in Giur. It, 2014, 990; SOANA, Le Sezioni Unite pongono limiti alla confisca nei confronti delle persone giuridiche per i reati tributari, in Riv. Giur. Trib., 2014, 388; CARDONE – PONTIERI, Il sequestro preventivo finalizzato alla confisca dei beni della società per delitti tributari commessi dal legale rappresentante, in Riv. Dir. Trib., 2014, 3, 53.
Il tema e la decisione sono stati esaminati nelle circolari n. 3 e 4, alla cui lettura dunque si rimanda.

Fallimento dell'ente e misure cautelari

La decisione

Sequestro preventivo nei confronti di una società – Successiva apertura di una procedura concorsuale – Mantenimento del sequestro – Sussistenza - Confisca – Ammissibilità (C.p.p., art. 321; d.lgs. n. 231 del 2001, art. 19, 53)

E' legittimo il mantenimento del sequestro preventivo finalizzato alla confisca di beni di una società nei cui confronti pende un procedimento per responsabilità amministrativa da reato anche quando sopravviene a carico dell'ente una procedura concorsuale, poiché tale vicenda non sottrae al giudice penale il potere di valutare, all'esito del procedimento, se disporre la confisca e, in caso positivo, con quale estensione e limiti (1).

CASSAZIONE PENALE – SEZIONE SECONDA – C.C. 11 GIUGNO 2015, N. 41354 (DEP. 14 OTTOBRE 2015) – ESPOSITO, PRESIDENTE – VERGA, ESTENSORE – FODARONI P.M. (CONF.) – IMET S.P.A.

(1) 1. Da tempo si prospetta il dubbio di quale disciplina applicare allorquando in sede di giudizio ex d.lgs. n. 231 del 2001 vengano assunti – o a titolo di sanzione definitiva o in sede cautelare – provvedimenti di vincolo sul patrimonio della persona giuridica sotto processo e l'ente colpito da tali provvedimenti viene nel frattempo – o sia stato in precedenza - dichiarato fallito o sottoposto ad altra procedura concorsuale. In tale circostanza, infatti, allora la confisca o il sequestro preventivo andranno ad incidere (non più su disponibilità economiche della società, quanto) su beni di pertinenza della massa attiva della procedura concorsuale, alla quale – proprio in ragione di quei provvedimenti giurisdizionali – sarà precluso il raggiungimento degli obiettivi e delle finalità che gli sono propri ed in particolare la liquidazione al miglior prezzo del patrimonio sociale ed il soddisfacimento dei creditori.
Ecco dunque che si affaccia un quesito la cui risoluzione da tempo affanna la giurisprudenza ovvero se il giudice, in sede di giudizio nei confronti dell'ente collettivo, ritenga di dover confiscare o sottoporre a sequestro preventivo beni di pertinenza della massa attiva di un fallimento, possa limitarsi ad accertare la confiscabilità dei cespiti, senza prendere in

considerazione le esigenze tutelate dalla procedura concorsuale, o debba invece procedere ad una valutazione comparativa tra le ragioni di questa - e segnatamente dei creditori in buona fede - e quelle afferenti alla pretesa punitiva dello Stato. A tale quesito, peraltro, da tempo se ne accompagna un altro, giacché fra quanti ritengono necessario un contemperamento fra le contrapposte esigenze della procedura concorsuale e dell'osservanza del dettato contenuto nel d.lgs. n. 231 del 2001 si discute se tale valutazione vada operata dal giudice penale o dal giudice fallimentare.

2. Sulla questione si sono pronunciate due volte le Sezioni Unite.
Con la pronuncia a Sezioni Unite del 24 maggio 2004 n. 29951, ricorrente Focarelli, si verificò – prescindendo dall'applicazione del dettato contenuto nel d.lgs. n. 231 del 2001 –se fosse consentito il sequestro preventivo finalizzato alla confisca facoltativa di beni provento di attività illecita dell'indagato e di pertinenza di impresa dichiarata fallita. Le Sezioni Unite affermarono che, pur in mancanza di una previsione legislativa, non poteva comunque sostenersi la radicale insensibilità del sequestro alla procedura concorsuale, affidando al potere discrezionale del giudice la conciliazione dei contrapposti interessi, ovvero di quelli propri della tutela penale (impedire che i proventi di illecito potessero giovare all'indagato) e di quelli tipici della procedura concorsuale (tutela dei legittimi interessi dei creditori nella procedura fallimentare).
Secondo le Sezioni Unite, quindi, il sequestro penale di beni di pertinenza di una massa fallimentare sarebbe senz'altro possibile, ma in tali casi il giudice penale deve dare motivatamente conto della prevalenza delle ragioni sottese alla confisca – e quindi all'adozione del previo sequestro cautelare - rispetto a quelle attinenti alla tutela dei legittimi interessi dei creditori e ciò in quanto gli interessi perseguiti dalla procedura concorsuale hanno anch'essi una natura pubblicistica – come desumibile dal ruolo del curatore fallimentare, quale emerge dalle fonti del suo potere, dalle finalità istituzionalmente collegate al suo agire e dai controlli che presidiano la sua attività gestoria, e che non deve essere considerato come un soggetto privato che agisca in rappresentanza o sostituzione del fallito o dei creditori, ma piuttosto come organo che svolge una funzione pubblica nell'ambito della amministrazione della giustizia, incardinato nell'ufficio fallimentare a fianco del tribunale e del giudice delegato.

3. Successivamente ed assai più di recente è da registrare la sentenza delle Sezioni Unite n. 11170 del 2015, con cui si previsto che quando il giudice ritenga di dover confiscare o sottoporre a sequestro preventivo beni di pertinenza della massa attiva di un fallimento, non si possano non considerare i diritti "dei terzi di buona fede", riservando tale valutazione al giudice penale che decide del processo ex d.lgs. n. 231 ovvero al giudice penale in sede di incidente di esecuzione.
In particolare, se da un lato la confisca del prezzo o del profitto del reato prevista dal citato art. 19, commi 1 e 2, deve essere obbligatoriamente adottato dal giudice penale abbia accertato la responsabilità dell'ente per l'illecito contestatogli al contempo la sanzione della confisca – ed eventualmente il sequestro cautelare – non potrà comunque avere ad oggetto beni in precedenza rientranti nel patrimonio dell'ente giudicato responsabile ma su cui nel frattempo terzi estranei all'illecito abbiano acquisito in buona fede un diritto reale. Di conseguenza, compete al giudice penale che decide del procedimento ex d.lgs. n. 231 del 2001 verso la società contemperare i diversi interessi – quelli connessi alla procedura punitiva di cui al citato decreto e quelli facenti capo ai terzi estranei.
In particolare, sarà il giudice penale a dover valutare se eventuali diritti vantati da terzi siano o meno stati acquisiti in buona fede e in caso di esito positivo di tale verifica il bene, la cui titolarità sia vantata da un terzo, non potrà essere sottoposto né a sequestro né a confisca, mentre qualora la posizione del terzo estraneo – o meglio l'esistenza dei diritti di questi - non sia emersa in precedenza, ovvero nel corso del procedimento nei confronti della società – ad esempio perché il terzo non era al corrente del procedimento in corso in danno dell'ente, la tutela del suo diritto potrà essere richiesta dallo stesso, a mezzo di apposita istanza al giudice dell'esecuzione penale.

4. In dottrina, sull'argomento MASSARI, Note minime in materiali sequestro probatorio sui beni del fallito, in Giur. It., 2005, 1507; IACOVIELLO, Fallimento e sequestri penali, in Fall., 2005, 1265; COMPAGNA, Obbligatorietà della confisca di valore e profili di discrezionalità nell'eventuale sequestro: il necessario contemperamento degli interessi costituzionali in gioco e l'ipotesi di fallimento, in Cass. Pen., 2009, 3034; SANTORIELLO, Procedura fallimentare e responsabilità degli enti: un rapporto ancora problematico, in Riv. Resp. Amm. Enti, 3-2015

Falso in bilancio ed interesse dell'ente

La decisione

Falso in bilancio – Responsabilità della società – Sussistenza dell'interesse o vantaggio – Individuazione del beneficio ottenuto dalla persona giuridica – Motivazione analitica - Necessità (C.c., art. 2621; d.lgs. n.231 del 2001, artt. 5, 6)

Il reato di falso in bilancio può sicuramente essere realizzato nell'interesse della società da cui proviene la comunicazione contabile e quindi dar luogo a una responsabilità da reato della stessa, ma è necessario che il giudice, nel pronunciare sentenza di condanna, individui chiaramente quale beneficio ha ricavato l'ente dalla condotta criminosa e motivi adeguatamente sul punto (1).

CASSAZIONE PENALE – SEZIONE PRIMA – C.C. 26 GIUGNO 2015, N.43689 (DEP. 29 OTTOBRE 2015), N. 43689 – GIORDANO, PRESIDENTE – TONI NOVIK, ESTENSORE – FIERONI P.M. (PARZ. DIFF.) – FENUCCI

(1) 1. Della sentenza in commento sorprende, da un lato l'ovvietà della massima e dall'altro - per quanto può comprendersi dalla lettura della pronuncia - la confusione in cui è incorso il giudice di merito.

2. Per comprendere quanto andiamo dicendo è il caso di ricostruire sinteticamente la vicenda di fatto.
Nei confronti degli amministratori di una società calcistica veniva mossa l'accusa di falso in bilancio ed al contempo si rinveniva un'ipotesi di responsabilità della persona giuridica in quanto il mendacio contabile sarebbe stato commesso l'interesse di questa, posto che il falso sarebbe stato diretto ad ottenere un abbattimento dei ricavi e quindi un pagamento di minori imposte. In una prima decisione, la Cassazione annullava con rinvio la condanna perché il giudice di merito non aveva adeguatamente motivato in ordine alla sussistenza del requisito dell'interesse dell'ente; il giudice di merito, in sede di giudizio di rinvio, confermava la condanna asserendo in maniera apodittica che le alterazioni contabili erano finalizzate al suddetto illecito risparmio d'imposta.

3. La nuova decisione della Cassazione annulla senza rinvio anche la seconda condanna evidenziando la superficialità della relativa motivazione. Non solo il giudice di merito non aveva fatto motivato in ordine alla sussistenza dell'interesse rinvenibile in capo alla società, ma era pervenuto ad una conclusione paradossale.
Nella decisione di merito, infatti, si afferma che il falso in bilancio era finalizzato ad un abbattimento dell'imponibile; di contro, il falso contabile contestato aveva determinato il maturare a vantaggio dell'ente di una serie di plusvalenze, l'emergere delle quali comportava evidentemente un aumento (e non un abbattimento) dell'imposta da versare, di modo che la conclusione con cui il giudice di merito giustificava la sua decisione di condanna era evidentemente contraddittoria.

4. L'interesse della decisione - che annulla senza rinvio la decisione del giudice di merito - è rinvenibile nella circostanza che la Cassazione, con un obiter dictum, indica quale può essere l'interesse che una società persegue nell'esporre falsamente i risultati della propria attività evidenziando come accanto alla finalità di evasione d'imposta può ricorrere l'ipotesi in cui la condotta criminale sia diretta ad "abbellire" il quadro economico e finanziario dell'ente - circostanza questa che si verifica di frequente quando, come nel caso di specie, la persona giuridica sia società per azioni quotata in borsa.
Evidentemente, laddove si voglia pervenire ad una decisione di condanna il giudice deve specificatamente indicare quale interesse della società sia stato soddisfatto, non essendo sufficiente indicare un generico beneficio economico che l'ente ha tratto la vicenda, dovendosi peraltro distinguere attentamente la circostanza in cui il reato sia stato posto in essere nell'interesse della persona giuridica dal caso in cui quest'ultima abbia ottenuto dal fatto un mero vantaggio. Laddove ricorra tale seconda ipotesi, infatti, sarebbe ben possibile che il vantaggio che l'ente ha ottenuto sia una conseguenza assolutamente casuale di una condotta che altri hanno tenuto nel loro esclusivo interesse, nel quale caso l'ente non potrebbe essere ritenuto responsabile ai sensi dell'art. 5, comma 2, d.lgs. n. 231 del 2001.

INFORMATICA FORENSE

di Giuseppe Vaciago, avvocato in Milano, e Giuseppe Dezzani, Digital Forensic Bureau, Torino

Le nuove norme sui controlli a distanza

La norma in vigore fino all' 11 Giugno scorso prevedeva il divieto di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Era possibile l'installazione di impianti e apparecchiature di controllo necessarie per esigenze organizzative e produttive, o per esigenza di sicurezza del lavoro, solo dopo un accordo con le rappresentanze sindacali, nei casi in cui dall'impiego degli strumenti potesse derivare anche una funzione di controllo a distanza.

Il testo approvato l' 11 Giugno prevede invece che l'"Accordo sindacale o autorizzazione ministeriale non sono necessari per l'assegnazione ai lavoratori degli strumenti utilizzati per rendere la prestazione lavorativa, pur se dagli stessi derivi anche la possibilità di un controllo a distanza del lavoratore".

Da un punto di vista tecnico l'esigenza nasce dal fatto che era praticamente impossibile impiegare uno strumento informatico e/o telematico senza che emergessero coinvolgimenti sindacali. Ogni strumento di fatto si presta ad un'attività di controllo remoto, anche in tempo reale. Il ragionamento del Governo è stato che ora non si deve più chiedere il permesso ai rappresentanti dei lavoratori per dotare un proprio dipendente di uno strumenti di lavoro quali sono diventati i computer o i dispositivi mobile. La sottile linea di demarcazione, ora spostata completamente a favore del datore di lavoro, viene tracciata dall'esigenza per cui viene dotato un dipendente di uno strumento hardware o software. Ovviamente nulla può ledere i principi della privacy, per cui il dipendente deve sempre essere informato di come vengono trattati i dati. In base alla nuova interpretazione di può procedere all'installazione di tutto ciò che sia indirizzato a perseguire il business aziendale, dotando il dipendente di tutto ciò che viene ritenuto necessario, anche dove lo strumento dovesse prestarsi ad verifica dell'efficienza lavorativa. Per cui, mentre prima anche per un dispositivo essenziale alla produzione era necessario ottenere l'accordo sindacale, ora non sarà più necessario. Ovviamente tale dispositivo non potrà mai essere

utilizzato con la sola finalità di controllo, ma essere solo una conseguenza dell'impiego dei dati che il sistema adottato mette a disposizione del datore di lavoro per la sua regolare attività lavorativa.

L'azienda potrà valutare i tabulati telefonici di un apparato dato in dotazione ad un dipendente, permettendo oltre ad una valutazione dei costi o delle direttrici di traffico, anche una valutazione di efficienza. Non ci sarà più alcun problema nell'adottare sistemi di controllo presenze o di valutazione di tempi e metodi (controlli a bordo macchina su tempi di produzione). Infine, non ci saranno più difficoltà ad installare software o sistemi di connessione dati che traccino le attività svolte, sempre partendo da un principio per cui si tratti di sistemi necessari allo svolgimento dell'attività lavorativa e non solo indirizzati al controllo.

Da un punto di vista giuridico, dunque, il secondo comma dell'art. 4 dello Statuto, così come modificato dall'entrata in vigore del d.lgs. 151/2015 (facente parte del più ampio pacchetto di riforme denominato "Jobs Act") introduce una deroga al citato preesistente divieto per quanto riguarda i c.d. "controlli preterintenzionali", che possono essere implicati come conseguenza indiretta dall'impiego di «impianti e apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro».

Ora, se da un lato, con la riforma in questione, è stato recepito anche a livello normativo il famoso orientamento giurisprudenziale dei controlli difensivi relativi all'accertamento delle condotte illecite realizzate dal lavoratore ed estranee al mero inadempimento, dall'altro con l'aggiunta della categoria relativa agli "altri strumenti dai quali derivi anche la possibilità di controlli a distanza dell'attività dei lavoratori" (cfr. art. 23 d.lgs. 151/2015), si è operato quell'adeguamento necessario ai tempi di oggi e anche al futuro, in quanto, essendo una formula aperta e generica può applicarsi ad un novero illimitato di mezzi tecnologici già esistenti, come anche a tutti quelli che verranno ad esistenza prossimamente.

La novità più importante della riforma, tuttavia, pare essere quella disposta nei commi successivi del già citato art. 23: "La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte ai sensi dei commi 1 e 2 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".

Se è vero, infatti, che attualmente il datore di lavoro può dotare i propri lavoratori degli strumenti tecnologici più disparati per lo svolgimento dell'attività lavorativa (si pensi agli smartphones, ai tablet od ai GPS aziendali) o di badges per il tracciamento delle presenze, senza che sia necessaria alcuna autorizzazione da parte delle rappresentanze sindacali, sembra ugualmente lecito che egli, avendone preventivamente informato i dipendenti, raccolga i dati originati da tali strumenti, compresi, quindi, anche quelli disciplinari o di corretto svolgimento delle proprio mansioni aziendali, di fatto perpetrando, in buona sostanza, un controllo del lavoratore mediante gli stessi.

In conclusione, nel caso in cui voglia usare sistemi di controllo a distanza, il datore di lavoro dovrà oggi anche aver informato adeguatamente il lavoratore e rispettato comunque le ulteriori disposizioni previste dal d.lgs. 196/2003 a tutela della privacy.

PRIVACY

di Patrizia Ghini, dottore commercialista e pubblicista in Milano

Poteri dell'Organismo di Vigilanza e informazioni coperte da segreto professionale

L'ente può trattare diversi tipi di informazioni, talune delle quali possono essere di natura confidenziale per previsione di legge o per una valutazione discrezionale dell'ente stesso o di una terza parte.
Per previsione di legge, sono riservati i "dati personali", secondo la definizione contenuta nell'art. 4 del d.lgs. 30.6.2003, n. 196 ("Codice in materia di protezione dei dati personali", di seguito Codice privacy).
Ad essi il Codice privacy attribuisce una specifica tutela, imponendo ai Titolari del trattamento, pubblici e privati, l'adozione di una serie di cautele, che vanno dall'obbligo di Informativa nei confronti degli interessati (le persone cui i dati si riferiscono), fino all'adozione di misure di sicurezza a protezione dei dati.

A particolari tipologie di dati personali, tra cui quelli sensibili di natura sanitaria (dati idonei a rivelare lo stato di salute), il Codice privacy riconosce maggiori tutele. Tra queste, la necessità di preventivo consenso degli interessati, l'adozione di più stringenti misure di sicurezza (maggiori, di regola, rispetto a quelle da adottare per proteggere i dati personali comuni). Nell'ambito degli enti che effettuano nella propria attività tipica diffusi "trattamenti di dati personali" (es. organismi sanitari, medici) sono richieste cautele ancora superiori, tra cui l'obbligo di gestire i dati sanitari nel rispetto del segreto professionale.
Tutto ciò premesso, si tratta di capire se l'Organismo di Vigilanza ai sensi del d.lgs. 231/01 abbia, nello svolgimento dei suoi compiti di vigilanza, il potere di accedere a documenti (cartacei o informatici) che contengono tali tipi di dati o se, viceversa, l'ente possa legittimamente rifiutarne o condizionarne l'accesso, anche in base al settore di appartenenza.

Per esaminare la questione, su un piano interpretativo appare utile partire dal principio di necessità di cui all'art. 3 del Codice privacy, il quale statuisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli

casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".
Tale principio (generale) trova una sua specificazione nell'art. 22, comma 6 del Codice privacy, dove è previsto che "i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".

Il settimo comma dell'art. 22 prevede poi un particolare obbligo di separazione dei dati sanitari, disponendo che "i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici".
L'art. 22 sopra richiamato è collocato nel Capo II, espressamente riferito ai soggetti pubblici, per i quali, quindi, il legislatore ha previsto e identificato specifiche misure di protezione obbligatorie.
Il punto 24 dell'Allegato B al Codice privacy statuisce a sua volta che "gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati".
Anche la "regola" appena richiamata non è espressamente riferibile alla generalità delle imprese, ma solo ad organismi sanitari ed esercenti professioni sanitarie (es. Asl, medici).

Pertanto sembra corretto sostenere che, per la generalità delle imprese, i dati sensibili sanitari andranno protetti, al minimo, mediate il trattamento separato degli stessi dagli altri dati personali; tale trattamento disgiunto potrà avvenire con svariate modalità, tra cui, ai massimi livelli, per imprese private in cui il trattamento dei dati sanitari ha una particolare rilevanza, come le Compagnie assicurative, la cifratura dei dati sensibili o l'utilizzo di

codici identificativi. La cifratura (o le relative modalità alternative) di cui all'art. 22, co. 6, infatti, è intesa come una delle possibili forme di trattamento disgiunto dei dati sensibili sanitari dai dati identificativi, applicabile obbligatoriamente in determinati ambiti (es. organismi sanitari). In altri settori, può comunque essere un parametro facoltativo per individuare le misure idonee di sicurezza.
In relazione alle imprese private del settore assicurativo, in cui il trattamento dei dati sanitari è particolarmente rilevante (si pensi ai dati necessari alla valutazione dello stato di salute dell'assicurando in una polizza sanitaria/vita) può essere utile osservare che anni fa il Garante privacy aveva richiamato l'opportunità di fare riferimento alle considerazioni espresse dal Consiglio d'Europa in una propria Raccomandazione (Rec (2002/9) che si focalizzava sulla protezione dei dati personali raccolti e trattati per scopi assicurativi. Da detta Raccomandazione si può rilevare quanto segue:

- fra le misure di sicurezza idonee che i titolari sono tenuti a adottare, vengono comprese quelle finalizzate ad evitare, in particolare, la commistione fra dati identificativi degli interessati, dati amministrativi e dati sensibili/sanitari; in sostanza, deve essere possibile accedere in modo separato a tali categorie di dati, evitando che l'accesso a documenti contenenti dati comuni comporti inevitabilmente anche l'accesso ai dati sensibili;
- la raccolta e le altre operazioni di trattamento di dati relativi allo stato di salute per scopi assicurativi, dovrebbe essere limitata a soggetti che appartengono al settore sanitario e, in ogni caso (quindi anche in quello che concerne le imprese assicurative), dovrebbe essere condizionata dal rispetto di principi di segretezza paragonabili a quelli cui soggiacciono gli operatori del settore sanitario.

E' utile evidenziare che in base all'art. 4, comma 1, lettera a), del Codice privacy con il termine "trattamento" ci si riferisce anche alla consultazione dei dati registrati/archiviati.

Alla luce delle considerazioni che precedono, sembra potersi desumere che, soprattutto in determinati enti, la gestione di documenti contenenti dati sanitari deve tenere conto dell'obbligo di "segretezza" per i dati stessi, che devono perciò essere segregati e ad accesso selezionato. Proprio in tali enti, tuttavia, l'attività di controllo dell'OdV potrebbe "incrociare" documenti contenenti informazioni di siffatta natura. C'è da chiedersi se, ove ciò

avvenga, vi sia una violazione del commentato obbligo di segreto professionale, considerato che, in ogni caso, l'OdV ha comunque un obbligo di riservatezza sulle informazioni apprese nello svolgimento dei suoi compiti.

Al riguardo, su un piano interpretativo si può notare che la differenza tra riservatezza e segreto è stata configurata da molti come una differenza di grado del bene tutelato. La distinzione viene individuata contrapponendo l'interesse al segreto, vale a dire ad impedire che terzi vengano a conoscenza della notizia, e l'interesse alla riservatezza, vale a dire a condizionarne la comunicazione, divulgazione e la pubblicizzazione della notizia stessa.
La notizia resta segreta anche se conosciuta da più soggetti, purché essi siano esattamente individuati o individuabili in ogni momento, potendosi, così, per contro, risalire agli "altri", cioè i terzi estranei. Questo, invece, non accade necessariamente per le notizie riservate, poiché esse possono essere conosciute, pur rimanendo riservate, anche da persone non esattamente individuabili, in quanto appartenenti ad una cerchia che può cambiare col tempo e che risulta qualificata da determinati rapporti con il soggetto titolare dei dati (es. rapporti economici, come quelli di lavoro dipendente, ecc.).
I confini della riservatezza appaiono, pertanto, mano netti rispetto a quelli del segreto, anche se ciò non esime il titolare del trattamento dall'obbligo di indicare chiaramente agli interessati, nell'informativa ex art. 13, Codice privacy, i soggetti ai quali le informazioni possono essere eventualmente comunicate, nonché l'ambito di eventuale diffusione delle stesse.
In altri termini, per ciò che riguarda l'interesse della persona, nel caso del "segreto" esso viene soddisfatto mantenendo immutata la situazione di fatto, cioè impedendo che venga a conoscenza del segreto chi non ne è partecipe in prima battuta (ad esempio, la compagnia assicurativa cui l'assicurato ha trasmesso i dati relativi al proprio stato di salute, attraverso la compilazione di appositi questionari o simili).

In conclusione, sembra che si possa affermare che l'ente (pubblico o privato, del settore sanitario o meno) deve evitare che l'Organismo di Vigilanza possa, nello svolgimento dei suoi compiti, accedere a documenti contenenti dati sanitari. Detta tipologia di dati andrebbe preventivamente oscurata (rendendoli anonimi, in quanto non riferibili a persona identificata o identificabile) oppure a priori collocata in separati documenti che,

nemmeno per caso fortuito, possano costituire oggetto di accesso o analisi da parte dell'OdV, in quanto, di massima, del tutto estranei all'attività di vigilanza che gli è demandata (anche nel caso in cui si tratti dell'OdV di un organismo sanitario, pubblico o privato).

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

L'Italia implementa gli alti principi in materia di beneficial ownership transparency, adottati nel 2014 dal gruppo di lavoro anticorruzione del G20

Come noto, l'Italia, in ambito ACWG del G 20 si è resa promotrice di *high principles on beneficial ownership transparency*, adottati proprio a Roma nel 2014, presso la Farnesina.
Si tratta di regole generali e condivise globalmente sulla trasparenza della titolarità societarie.
Si è ora nella fase dell'attuazione in ciascun ordinamento delle regole suddette: Paesi come Regno Unito e India hanno già provveduto.
In vista dei prossimi impegni dell'Italia sono in fase di preparazione i criteri di delega per il recepimento della IV direttiva antiriciclaggio pubblicata in GUCE il 5.06.15 (in vigore dal 25 giugno).

Due articoli della direttiva sono proprio relativi alla trasparenza della titolarità effettiva: l'art. 30 (per le persone giuridiche) e l'art. 31 (per i trust). Gli stessi impongono agli Stati membri di custodire le informazioni in un registro centrale che nel caso italiano sarà implementato da Infocamere.

SOCIETÀ ED ENTI PUBBLICI

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

Pubblica amministrazione e antiriciclaggio: gli indicatori di anomalia

Il decreto del Ministro dell'interno 25 settembre 2015 (G.U. n. 233 del 07.10.2015), a oggetto: "Determinazione degli indicatori di anomalia al fine di agevolare l'individuazione delle operazioni sospette di riciclaggio e di finanziamento del terrorismo da parte degli uffici della pubblica amministrazione" (dopo solo "decreto"), rappresenta un ulteriore tassello per l'applicazione del decreto legislativo 21 novembre 2007, n. 231: "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio[1] dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e successive modificazioni e integrazioni. Un decreto analogo del 17 febbraio 2011 aveva determinato gli indicatori di anomalia per agevolare l'individuazione delle operazioni sospette di riciclaggio da parte di alcune categorie di operatori non finanziari. L'attuale decreto – che interviene otto anni dopo l'emanazione del decreto legislativo 231/2007 – ha lo stesso scopo, rivolgendosi però alle amministrazioni pubbliche.

Occorre, infatti, ricordare che l'articolo 10, comma 2, lettera g), del decreto legislativo 231/2007 prevede, tra i destinatari degli obblighi di segnalazione

[1] L'art. 2, comma 1, del d. lgs 231/2007 recita: "Ai soli fini del presente decreto, le seguenti azioni, se commesse intenzionalmente, costituiscono riciclaggio: a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) la partecipazione a uno degli atti di cui alle lettere precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione".

di operazioni sospette, gli uffici della pubblica amministrazione. L'articolo 66, comma 4, dello stesso decreto stabilisce poi che la definizione di pubblica amministrazione – prevista dall'articolo 1, comma 2, lettera r), sempre del decreto 231/2007 – sia modificata con decreto del Ministro dell'economia e delle finanze di concerto con il Ministro per le riforme e le innovazioni nella pubblica amministrazione. Il decreto in esame, richiamando queste disposizioni, precisa (art. 1 co. 1, lett. h) che, per "uffici della pubblica amministrazione", s'intendono "tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado, le istituzioni educative, le aziende e le amministrazioni dello Stato a ordinamento autonomo, le regioni, le province, i comuni, le comunità montane e loro consorzi e associazioni, le istituzioni universitarie, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale, le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300, nonché le città metropolitane di cui all'art. 1 della legge 7 aprile 2014, n. 56". In buona sostanza tutti questi soggetti, "quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo", devono segnalare (art. 41, co. 1, d.lgs. 231/2007) queste situazioni all'UIF, l'Unità di informazione finanziaria per l'Italia istituita presso la Banca d'Italia (art. 6 d.lgs. 231/2007) a prescindere dal relativo importo. L'articolo 7 del decreto detta le modalità con le quali gli uffici della pubblica amministrazione devono effettuare la segnalazione all'UIF. La segnalazione è trasmessa, senza ritardo, in via telematica.

Il decreto puntualizza che il sospetto deve fondarsi su una compiuta valutazione degli elementi oggettivi e soggettivi dell'operazione all'esame. Gli indicatori di anomalia aiutano nelle analisi da effettuare sulle operazioni. Infatti, essi sono "volti a ridurre i margini di incertezza connessi con valutazioni soggettive" allo scopo di "contribuire al contenimento degli oneri e al corretto e omogeneo adempimento degli obblighi di segnalazione di operazioni sospette". Le operazioni compiute dalle amministrazioni pubbliche che possono destare i sospetti sono quelle riferite a un "soggetto (persona fisica o entità giuridica) nei cui confronti gli uffici della pubblica amministrazione svolgono un'attività finalizzata a realizzare un'operazione a contenuto economico, connessa con la trasmissione o la movimentazione di mezzi di pagamento o con la realizzazione di un obiettivo di natura finanziaria o patrimoniale ovvero nei cui confronti sono svolti controlli di competenza degli uffici medesimi" (art. 2, co. 2, decreto).

L'allegato al decreto elenca, in maniera molto dettagliata ancorché non esaustiva, gli "indicatori di anomalia" distinti in:

a) indicatori di anomalia connessi con l'identità o il comportamento del soggetto cui è riferita l'operazione;
b) indicatori di anomalia connessi con le modalità (di richiesta o esecuzione) delle operazioni;
c) indicatori specifici per settore di attività, suddivisi per: controlli fiscali, appalti, finanziamenti pubblici, immobili e commercio.

All'articolo 6, il decreto indica le procedure interne che le amministrazioni pubbliche devono seguire per rendere operativo il sistema delle segnalazioni all'UIF. È previsto un soggetto cui gli addetti agli uffici della pubblica amministrazione trasmettono le informazioni rilevanti ai fini della valutazione delle operazioni sospette. Questo soggetto, denominato "gestore", può coincidere con il responsabile della prevenzione della corruzione previsto dall'articolo 1, comma 7, della legge 190/2012. Qualora i due soggetti non coincidano, gli enti devono prevedere adeguati meccanismi di coordinamento tra i medesimi. Le amministrazioni pubbliche devono, inoltre, curare l' "adeguata formazione del personale e dei collaboratori ai fini della corretta individuazione degli elementi di sospetto" (art. 8 decreto).

Anche ad una rapida lettura, non sfugge l'enorme dimensione della materia trattata dal decreto, con implicazioni che spaziano dagli aspetti e competenze professionali dei dipendenti pubblici che dovrebbero curarne l'applicazione, a quelli organizzativi degli enti sotto il profilo delle infrastrutture tecnologiche e per l'impostazione di sistemi di raccolta degli elementi occorrenti per la valutazione delle operazioni, nei quali rientrano anche le informazioni sul soggetto cui è riferita l'operazione "acquisite nell'ambito dell'attività svolta, e in particolare di quelle inerenti a persone politicamente esposte, soggetti inquisiti o censiti nelle liste pubbliche di terrorismo" (art. 6, co. 11, decreto). Senza trascurare le risorse finanziarie che andrebbero impegnate per compiere quanto il decreto prevede.

Visto nel complesso e astrattamente, il decreto può certamente apparire come uno strumento di grande efficacia nel contrasto al riciclaggio e al finanziamento del terrorismo. Perplessità tuttavia sorgono circa la possibilità di una concreta applicazione delle norme che esso reca. Intanto, è comunque una pecca genetica che venga alla luce dopo otto anni

dall'emanazione del decreto legislativo 231/2007. Se lotta al riciclaggio e al finanziamento del terrorismo ha da farsi, gli strumenti vanno predisposti tempestivamente. Tenendo conto di questo fatto, può quasi apparire pleonastico che ora si disponga che le amministrazioni devono procedere alle segnalazioni "senza ritardo" (e senza dire dell'ambiguità sempre presente in queste formulazioni).

Il decreto costruisce poi un impianto corposo cui le amministrazioni pubbliche dovrebbero attenersi per contribuire alla lotta al riciclaggio e al finanziamento del terrorismo. Va però osservato che sfugge tanto nel decreto 231/2007 quanto nelle norme del decreto all'esame l'aspetto sanzionatorio. In altre parole, se ci siano sanzioni applicabili agli uffici della pubblica amministrazione che non ottemperano agli obblighi di segnalazione e quali esse siano (è ormai ampiamente assodato che, se non sono previste sanzioni, le norme hanno un'elevata probabilità di non essere applicate). Una domanda banale – ma onnicomprensiva – è quella di chiedersi se la pubblica amministrazione possieda, da subito o anche a breve attraverso la formazione, la cultura per applicare le norme delle quali dovrebbe farsi carico nella lotta al riciclaggio. Ed inoltre, si può pensare come sia facile alibi – nell'attuale congiuntura negativa della finanza pubblica – osservare che mancano le risorse per impiantare il complesso sistema disegnato dal decreto.

Infine, non può dimenticarsi che andrebbe stabilito quali interazioni e correlazioni potrebbero crearsi tra decreto 231 del 2007 (e norme attuative) e decreto 231 del 2001, attesoché quest'ultimo annovera tra i reati presupposto (art. 25-octies) anche quello di riciclaggio.
Le note conclusive indicano dubbi ed incertezze che non sembrano trascurabili.