

Circolare(231)

approfondimenti, notizie e informazioni



n. 11 – dicembre 2015

PLENUM

rivista231.it

Sommario

| | |
|---|-----------|
| 1. AMBIENTE E SICUREZZA | 3 |
| <i>di Marina Zalin</i> | |
| 2. ANTIRICICLAGGIO E ANTICORRUZIONE | 5 |
| <i>di Ranieri Razzante</i> | |
| 3. GIURISPRUDENZA ANNOTATA | 7 |
| <i>di Ciro Santoriello</i> | |
| 4. ORGANISMO DI VIGILANZA | 10 |
| <i>di Patrizia Ghini e Luigi Fruscione</i> | |
| 5. PRIVACY | 13 |
| <i>di Patrizia Ghini</i> | |
| 6. PROFILI INTERNAZIONALI | 17 |
| <i>di Giovanni Tartaglia Polcini e Paola Porcelli</i> | |
| 7. SOCIETÀ ED ENTI PUBBLICI | 22 |
| <i>di Carlo Manacorda</i> | |

AMBIENTE E SICUREZZA

di Marina Zalin, Butti & Partners, Verona

Responsabilità amministrativa dell'ente e reati colposi di evento (Tribunale di Milano, sentenza 10647/15 bis, dr.ssa Canevini)

La vicenda fattuale sottesa al caso in esame è relativa alle gravi lesioni occorse a un lavoratore caduto da un trabattello, dall'altezza di circa 6 metri, ribaltatosi a causa del movimento di un carroponete che lo colpiva. Il lavoratore, intento nella manutenzione di una pompa di calore, riportava gravi fratture e traumi distorsivi importanti.

Le cause del sinistro, come contestate dal P.M., erano riconducibili a fatti di natura omissiva quali la mancata realizzazione del DUVRI (Documento unico di valutazione dei rischi interferenti) e la mancata adozione dei necessari presidi di sicurezza sui mezzi impiegati per la lavorazione, in particolare riferiti all'assenza di cunei ferma-ruote del trabattello.

La sentenza ricostruisce dapprima la natura della responsabilità amministrativa da reato dell'ente, precisando che si tratta di una forma nuova di colpevolezza per omissione organizzativa e gestionale direttamente imputabile all'ente stesso.

In seguito fa riferimento alla compatibilità del sistema con i reati colposi di evento, già oggetto di perplessità in seno alla dottrina: se l'evento lesivo non è voluto, sostengono alcuni, non è possibile che l'ente persegua il fine di conseguire un diretto vantaggio.

Il Giudice, tuttavia, mostra di aderire alla diversa corrente, argomentando sul punto che l'interesse o il vantaggio per l'ente non vanno considerati come parametri di valutazione soggettiva, bensì come effetto della condotta posta in essere dall'agente.

Va così valutato, in conseguenza, se la realizzazione del reato-presupposto (qui le lesioni colpose ex art. 590 c.p.) abbiano comportato interesse o vantaggio per l'ente, ovvero se sia stata foriera di esclusivo beneficio dell'agente o di terzi.

La sentenza ripercorre altresì la distinzione tra interesse e vantaggio, da valutarsi in modo autonomo: l'interesse può prescindere dall'effettivo conseguimento di un beneficio economico (in tal caso rimanendo solo

perseguito ma non ottenuto), così come il vantaggio può derivare pur in una totale assenza di prospettazione *ex ante*.

La pronuncia volge verso il termine dell'articolato ragionamento giuridico, ricostruttivo delle premesse logico-concettuali della responsabilità dell'ente, valutando nel caso concreto la sussistenza di un interesse o vantaggio per l'ente imputato ai sensi dell'art. 25-*septies*.

La violazione di norme cautelari deve configurare un vantaggio per l'ente, spesso riconosciuto in negativo sotto forma di risparmio economico (es. mancata adozione di presidi, contenimento dei costi) o anche in positivo sotto forma di migliore produttività o di velocizzazione del processo produttivo pur in presenza di rischio per la salute.

Nel caso considerato il Giudice meneghino ha ritenuto provato l'interesse attuale e diretto a svolgere i lavori in tempi ristretti, nonché il risparmio conseguente alla mancata adeguazione delle strumentazioni alle norme antinfortunistiche.

Ulteriore carenza è rappresentata dall'assenza del DUVRI relativo al rischio di interferenze tra le diverse imprese operanti congiuntamente, la cui mancanza è stata da un lato decisiva a produrre l'evento e dall'altra ha comportato un risparmio economico e una velocizzazione dei lavori, che era di palese interesse per l'ente.

Per tutte le ragioni sopra delineate il Giudice ha condannato l'ente alla pena base di 250 quote da €258 ciascuna, ridotta della metà per l'esiguità del risparmio di spesa e di tempo ai sensi dell'art. 12 co. 1 lett. a) ed ulteriormente ridotta di un terzo per la scelta del rito abbreviato.

ANTIRICICLAGGIO E ANTICORRUZIONE

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

Riciclaggio e valute virtuali

Nel Rapporto annuale 2015 IOCTA (*Internet Organised Crime Threat Assessment*), pubblicato da Europol, viene rilevato come le organizzazioni criminali internazionali (*Transnational Crime Organisations*) abbiano ormai spostato i propri traffici illeciti nel mondo virtuale grazie all'ausilio delle monete dematerializzate, in primo luogo i *Bitcoin*, che consentono di ottenere ingenti guadagni in una situazione di quasi totale assenza di controlli.

In particolare il *Bitcoin* viene definito dall'Europol come la principale moneta utilizzata dalla criminalità organizzata *on-line*, in special modo dai c.d. cyber-riciclatori, attraverso la quale vengono compiute innumerevoli attività illecite, quali riciclaggio, estorsione, traffico di droga, armi ed essere umani.

Per tali ragioni le forze dell'ordine sono state invitate a diffondere il più possibile il successo di eventuali iniziative repressive e, al contempo, condividere le conoscenze, le esperienze e le *best practices* su come affrontare l'utilizzo illecito dei *Bitcoin* e dei nuovi strumenti di pagamento digitale nel corso di indagini di tipo informatico.

Le valute virtuali - ossia le rappresentazioni in formato digitale del denaro - continuano ad essere infatti "attenzionate" da parte delle autorità inquirenti internazionali ed europee.

Le ragioni per cui le c.d. "*virtual currencies*" destano così grande preoccupazione e allarme possono essere racchiuse nelle loro tre principali caratteristiche: a) creazione privata; b) assenza di controlli da parte di istituzioni statali; c) anonimato.

Il sempre maggior utilizzo di tali valute non solo nel mondo del commercio informatico, ma soprattutto nell'ambito strettamente economico-finanziario, aveva già indotto l'Autorità Bancaria Europea (*European Banking Authority, EBA*) a pubblicare il 4 luglio 2014 il "Parere sulle Valute Virtuali" (*Opinion on Virtual Currencies*), dove venivano individuati i rischi in cui i singoli utenti sarebbero potuti incorrere nel caso di utilizzo di tali strumenti (furti di valuta

virtuale, riciclaggio, fallimento delle piattaforme di scambio), considerati ben più alti dei possibili benefici.

Queste preoccupazioni sono state confermate anche dal recente rapporto del FATF (*Financial Action Task Force*) o GAFI (Gruppo d'Azione Finanziaria Internazionale) del giugno 2015 intitolato "Linee guida per un Approccio Basato sul Rischio - Valute Virtuali" (*Guidance for a risk-based approach – Virtual Currencies*), ove viene precisato che la moneta virtuale "è una rappresentazione digitale di valore che può essere oggetto di scambio nel mercato digitale e può svolgere contemporaneamente le funzioni di: 1) mezzo di scambio; 2) unità di conto; 3) riserva di valore. Essa non ha corso legale in alcuna giurisdizione e non è rilasciata né garantita da alcuna autorità, e svolge le funzioni di cui sopra solamente previo accordo all'interno della comunità degli utenti che la utilizzano".

GIURISPRUDENZA ANNOTATA

di **Ciro Santoriello**, Sostituto Procuratore presso il Tribunale di Torino

Costituzione dell'ente ed esercizio del diritto di difesa

La decisione

Sentenza di condanna della persona giuridica - Impugnazione - Individuazione dei soggetti legittimati ad impugnare – Impugnazione della persona fisica autore del reato presupposto - Inammissibilità (D.lg. n. 71, 72)

Nomina del difensore di fiducia dell'ente – Nomina da parte del rappresentante legale indagato o imputato – Incompatibilità – Inefficacia della nomina – Conseguenze – Dichiarazione di contumacia dell'ente e nomina del difensore d'ufficio (D.lg. n. 231 del 2001, art. 39, 40, 41)

L'imputato autore del reato presupposto non è legittimato e non ha interesse ad impugnare, anche nel caso di simultaneus processus, il capo della sentenza relativa all'affermazione della responsabilità da reato dell'ente nel cui interesse o vantaggio lo stesso sia stato commesso, dovendosi individuare quali unico soggetto legittimato ad impugnare tale capo della sentenza il solo ente collettivo (1)

In materia di responsabilità da reato degli enti, il rappresentante legale indagato o imputato del reato presupposto non può provvedere, a causa di tale condizione di incompatibilità, alla nomina del difensore di fiducia dell'ente, per il generale e assoluto divieto di rappresentanza posto dall'articolo 39 del decreto legislativo 8 giugno 2001 n. 231. Laddove l'atto di costituzione dell'ente e la nomina del difensore e procuratore speciale vengano effettuati dal rappresentante legale incompatibile, stante l'inefficacia di tali atti, il giudice deve procedere alla dichiarazione di contumacia dell'ente e nominare allo stesso un difensore d'ufficio (2).

1. La particolare disciplina in tema di costituzione dell'ente collettivo nel processo nei suoi confronti continua a far discutere, anche se dopo la

decisione delle sezioni unite n. 15249 del 2015 (per un approfondimento della quale si rinvia alle newsletter del giugno e del settembre 2015) le incertezze sembrano debbano ritenersi superate, come espressamente affermato nella pronuncia in epigrafe.

2. In proposito si ricorda che la giurisprudenza ritiene che il legale rappresentante dell'ente, il quale sia a sua volta indagato per il reato presupposto, non può compiere alcun atto difensivo nell'interesse dell'ente e che laddove atti del genere vengono posti in essere gli stessi devono ritenersi inefficaci.

Si ricorda che secondo le sezioni unite, pure se la costituzione dell'ente collettivo nel processo non può essere effettuata se non facendo ricorso al particolare procedimento descritto dall'art. 39, comma 1, D.Lgs. n. 231/01, il sistema processuale delineato dal citato decreto consente comunque all'ente di nominare comunque un difensore di fiducia anche in assenza di una sua formale costituzione nel procedimento - da intendersi tale espressione come facente riferimento non solo alla fase del giudizio ma anche alla fase delle indagini preliminari.

Il motivo per cui la società non costituitasi può comunque legittimamente nominare un proprio difensore di fiducia è secondo la Corte di Cassazione duplice. In primo luogo, a sostegno di questa tesi sta un indice normativo rappresentato dal fatto che la stessa dichiarazione di costituzione dell'ente deve essere sottoscritta dal difensore ed è quindi un atto del difensore fiduciario: ciò inevitabilmente implica, che anche prima di tale costituzione, ben possa essere stata effettuata dal rappresentante legale dell'ente la nomina del difensore di fiducia.

In secondo luogo, la Corte invita a considerare come, in relazione a particolari atti investigativi - si pensi ai cosiddetti atti a sorpresa -, occorra riconoscere prontamente alla persona giuridica la possibilità di esercitare le proprie facoltà difensive, secondo le modalità che la stessa ritenga più opportune: sarebbe infatti lesivo dei diritti inviolabili di difesa propri dell'ente collettivo sottoposto a processo ritenere che al difensore di fiducia comunque nominato, sia pur senza previa costituzione ex art. 39 citato, non possa comunque far valere le ragioni della persona giuridica.

3. Questa conclusione però non vale nel caso in cui la nomina del difensore di fiducia provenga dalla rappresentante legale della società, il quale sia a sua volta indagato o imputato per il medesimo reato presupposto da cui discende l'eventuale responsabilità dell'ente collettivo.

In tale circostanza, l'inefficacia della nomina del difensore di fiducia non dipende dal fatto che l'ente, non essendosi costituito, non ha fatto ancora comparsa nel proscenio processuale, quanto dalla presunzione di incompatibilità che in questo caso sussiste fra l'ente collettivo ed il suo rappresentante legale, il quale essendo indagato o imputato per un illecito da cui deriva la responsabilità della persona giuridica presso cui egli stesso operava, si ritiene versare - con presunzione assoluta ed insuscettibile di prova in senso contrario - in una situazione di conflitto di interessi, che lo rende inidoneo ad esercitare qualsiasi facoltà difensiva per conto dell'ente. Ciò comporta quindi che, laddove il rappresentante legale indagato o imputato del reato presupposto abbia provveduto alla nomina del difensore di fiducia dell'ente, tale nomina è da ritenersi priva di qualsiasi efficacia ed eventuali istanze vanno qualificate come inammissibili.

ORGANISMO DI VIGILANZA

di **Patrizia Ghini, dottore commercialista e pubblicista in Milano, e Luigi Fruscione, avvocato in Roma**

Le riunioni periodiche dell'OdV: spunti operativi

Le funzioni attribuite all'Organismo di Vigilanza sono particolarmente complesse. Ci si rende conto della delicatezza delle stesse ogni giorno di più e di pari passo aumenta il senso di responsabilità nello svolgimento del delicato incarico.

L'Organismo ha una funzione di vigilanza all'interno di un sistema di prevenzione penale che ha quale destinatario naturale, anche se solo eventuale, l'Autorità giudiziaria penale; il Modello è destinato a venire in rilievo esclusivamente nel caso in cui si contesti un reato al soggetto collettivo nel rispetto dei requisiti indicati nella normativa di riferimento (artt. 5 e 6 del D.Lgs. n.231/01).

Avere ben chiaro il fatto che interlocutore dell'attività di vigilanza è il giudice penale aiuta a comprendere che l'attività di controllo va sviluppata il più possibile non con strumenti formali (ma poco sostanziali), bensì con l'effettiva volontà di contribuire a prevenire la commissione di reati.

In tale ottica, assume ruolo centrale nella difesa dell'ente il modus operandi dell'Organismo di Vigilanza, lo svolgimento effettivo e non meramente formale della vigilanza e la documentazione (non certo schematica) dell'attività svolta.

Per svolgere al meglio la propria funzione di vigilanza e, di fatto, contribuire nella prevenzione, a parere di chi scrive, dovrebbe essere intensificata l'attività sul campo e di relazione tra l'OdV e:

- le figure apicali;
- le figure poste a presidio di un processo a rischio;
- le funzioni di controllo interne, ove esistenti;
- gli organi di controllo esterni.

Gli incontri rappresentano un'occasione fondamentale per:

- coinvolgere le persone sul tema e favorire la circolazione delle informazioni;
- sensibilizzare e consigliare tali soggetti in merito agli obblighi (misure e procedure) derivanti dal Modello;

- sorvegliare e migliorare l'applicazione delle politiche 231, compresa l'attribuzione delle responsabilità, la formazione del personale e le attività di audit;
- verificare la conoscenza e l'applicazione effettiva del Modello e del Codice etico.
- avere piena consapevolezza della peculiarità della funzione di vigilanza affidatagli dall'organo dirigente;
- organizzare la propria attività sulle due direttrici della verifica dell'effettività e della verifica dell'adeguatezza del Modello.

Gli incontri e la verbalizzazione degli incontri rappresentano il miglior sistema per dimostrare che il Modello è vivente, non sulla carta.

Ne sottolineano l'importanza anche le Linee Guida Confindustria:

.... Il coinvolgimento, con riferimento alla salute e sicurezza dei lavoratori, dovrebbe essere realizzato attraverso:

- *la consultazione preventiva della RLS, ove presente, e del medico competente, ove previsto, in merito alla individuazione e valutazione dei rischi e alla definizione delle misure preventive;*
- *riunioni periodiche che tengano conto non solo delle richieste fissate dalla legislazione vigente, ma anche delle segnalazioni ricevute dai lavoratori e delle esigenze o problematiche operative riscontrate.*

Con riferimento ai reati ambientali, inoltre, la comunicazione ed il coinvolgimento dei soggetti interessati dovrebbero essere realizzati attraverso riunioni periodiche di tutte le figure competenti per la verifica della corretta gestione delle tematiche ambientali, a valle delle quali dovrebbe essere prevista un'adeguata diffusione dei risultati (ad es. prestazioni, incidenti e mancati incidenti ambientali) all'interno dell'organizzazione e, quindi, anche verso i lavoratori.

.... La circolazione delle informazioni all'interno dell'azienda assume un valore rilevante per favorire il coinvolgimento di tutti i soggetti interessati e consentire consapevolezza e impegno adeguati a tutti i livelli.

Il coinvolgimento, con riferimento alla salute e sicurezza dei lavoratori, dovrebbe essere realizzato attraverso:

- *la consultazione preventiva della RLS, ove presente, e del medico competente, ove previsto, in merito alla individuazione e valutazione dei rischi e alla definizione delle misure preventive;*

- *riunioni periodiche che tengano conto non solo delle richieste fissate dalla legislazione vigente, ma anche delle segnalazioni ricevute dai lavoratori e delle esigenze o problematiche operative riscontrate.*

Il sistema di prevenzione definito nel decreto 81/2008 attribuisce un ruolo decisivo alle riunioni periodiche di prevenzione e protezione rispetto ai rischi per salute e sicurezza sul lavoro, sanzionando gravemente la violazione dell'obbligo.

La riunione periodica costituisce un momento di confronto tra i soggetti chiave del sistema 231 sull'efficacia del programma di prevenzione adottato, soprattutto nelle PMI, dove spesso i quotidiani ritmi lavorativi portano a trascurare questo importante adempimento.

Il presente contributo presenta e giustifica una serie di interventi che si intende proporre dal 2016 sul tema per dare spunti o suggerimenti sugli argomenti da porre all'ordine del giorno delle riunioni periodiche dell'Organismo di Vigilanza, anche per contribuire ad assolvere il compito di aggiornare sull'evoluzione della normativa e compiere la valutazione di impatto in termini di aggiornamento del modello.

PRIVACY

di Patrizia Ghini, dottore commercialista e pubblicista in Milano

Arriva la riforma in materia di protezione di dati personali. Privacy e 231 sempre più simili nella metodologia applicativa

Dopo i negoziati tra le tre istituzioni europee (Commissione, Parlamento e Consiglio), proprio nei giorni scorsi è stato raggiunto l'accordo sulla riforma in materia di protezione dei personali. La riforma si compone di due strumenti:

il regolamento generale sulla protezione dei dati;

la direttiva sulla protezione dei dati trattati dalla polizia e dalle autorità giudiziarie penali.

Il Garante ha dato prontamente notizia dell'importante tappa raggiunta attraverso la pagina informativa consultabile al link <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361>.

The screenshot shows a web browser displaying the website of the Garante per la protezione dei dati personali. The page title is "Il nuovo \"pacchetto protezione dati\" - Pagina informativa". The main content area features a large heading "Il nuovo \"pacchetto protezione dati\" - Pagina informativa" and a sub-heading "Testi relativi aggiornati all'esito della prima lettura da parte di Parlamento e Consiglio UE". Below this, there is a "SCHEDA" section with the following details: "Doc-Web: 4443361" and "Data:". To the right of the "SCHEDA" section, there is a large orange and blue banner with the text "Il nuovo \"pacchetto protezione dati\": Proposta di Regolamento generale sulla protezione dei dati personali e Proposta di Direttiva sulla protezione dei dati personali nelle attività di contrasto". The page also includes a search bar, a navigation menu, and social media sharing options.

Come evidenziato nella scheda, “il 18 dicembre 2015 è stato raggiunto un accordo sul testo del Regolamento e della Direttiva, che sarà formalizzato nei primi mesi del 2016 dal Consiglio e dal Parlamento UE e culminerà con la pubblicazione nella Gazzetta Ufficiale.

Il pacchetto protezione dati sarà in vigore dalla primavera del 2018 (due anni di *vacatio*). Il testo è disponibile al momento solo in lingua inglese. Una traduzione non ufficiale potrà essere disponibile tra breve”.

Anche se le nuove norme saranno applicabili due anni dopo la loro pubblicazione, conviene muoversi per tempo nell’attuazione dei nuovi principi in quanto stimolano la creazione di un sistema di *compliance* effettivo e non meramente formale.

In particolare, sembra essenziale tenere già conto di alcune fondamentali novità, quali:

- il principio di “*accountability*” (rendicontazione);
- quello della “*Privacy by design*”;
- il criterio del “*Privacy impact assessment*” o del “*Data protection Impact Analysis*” (valutazione d’impatto) preventivo;
- i nuovi criteri per l’analisi dei rischi circa la sicurezza dei dati;
- i nuovi obblighi di segnalazione di violazione sui dati personali (c.d. “*personal data breach*”);
- la necessità di un ruolo proattivo da parte del “Titolare del trattamento”.

Alcuni dei principi introdotti dal Regolamento erano stati anticipati nelle Linee Guida Privacy OCSE riviste, rese ufficialmente disponibili sul sito dell’OCSE il 9 settembre 2013, adottate dal Consiglio OCSE l’11 luglio successivo. Tali Linee Guida costituivano il primo aggiornamento della versione del 1980 (*original 1980 version*), il primo accordo internazionale su principi condivisi in materia di *privacy*.

Due i temi che rappresentano il cuore delle Linee guida aggiornate, ma anche della riforma. Il primo di questi è proprio un *focus* sulla realizzazione pratica della protezione della *privacy*, attraverso un approccio fondato sulla gestione del rischio.

Le Linee guida fanno perno su una serie di concetti innovativi, tra cui:

- l’importanza strategica della *privacy*, che richiede, appunto, una “strategia” coordinata:

- i programmi di gestione della privacy, che servono come meccanismo operativo di base attraverso il quale i titolari del trattamento possono implementare la strategia *privacy* prescelta;
- la notifica della violazione della sicurezza dei dati, da trasmettere sia ad un'Autorità sia all'interessato.

In base alle citate Linee Guida, l'applicazione dei nuovi principi (*privacy by design, privacy by default, valutazione dei rischi, data breach*) rappresentano la condizione affinché lo sviluppo dell'ente sia attento ai dati e rispettoso delle tutele che vengono riconosciute dalla normativa.

Le novità sono molteplici ma quella più significativa riguarda la figura del Responsabile della protezione dei dati ("*Data Protection Officer*", *DPO*) prevista per il settore pubblico e, nel settore privato, per le grandi imprese o allorquando le attività principali consistono in trattamenti che richiedono il controllo regolare e sistematico degli interessati.

Tale soggetto rappresenta una figura fondamentale, da scegliere in funzione delle qualità professionali e della conoscenza specialistica della *privacy*.

Di fatto, i compiti propri di tale figura rappresentano le attività che, a parere di chi scrive, consentono di garantire una conformità effettiva (e non meramente formale) alla *privacy*:

- sensibilizzare e consigliare il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti dal Regolamento;
- sorvegliare l'applicazione delle politiche *privacy*, compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli *audit* connessi;
- sorvegliare l'applicazione del Regolamento, con particolare riguardo alla regola della protezione (dei dati) fin dalla progettazione (delle attività/operazioni aziendali), alla protezione di *default*, alla sicurezza dei dati, alle informazioni dell'interessato e alle richieste degli stessi per esercitare i diritti riconosciuti;
- controllare che il Titolare effettui la valutazione d'impatto sulla protezione dei dati (DPIA) e richieda all'Autorità l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- fungere da punto di contatto per l'Autorità su questioni connesse al trattamento dei dati personali e consultarla, se del caso, di propria iniziativa;
- informare i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

La riforma avvicina molto i due sistemi privacy e 231 non solo perché in entrambi si stimola la gestione del rischio in un'ottica di prevenzione, ma anche perché il successo del sistema di fatto viene affidato a delle figure (Odv e Responsabile della protezione dei dati personali) le cui competenze sono essenziali per consentire all'ente stesso di raggiungere l'impegnativo compito della conformità.

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

High level principles on private sector transparency and security: la nuova sfida del G20 anticorruzione per una 231 di livello globale

Al vertice G20 di Antalya, nel dicembre 2015 (15 e 16), nonostante l'emergenza terroristica ingenerata dai drammatici eventi di Parigi, i *leaders* dei Paesi più industrializzati hanno ratificato molti dei documenti adottati dai gruppi di lavoro nel corso dell'esercizio annuale.

Il Gruppo dei 20 (o G20) è un *Forum* creato nel 1999, dopo una successione di crisi finanziarie, al fine di favorire l'internazionalità economica e la concertazione, tenendo conto delle nuove economie in sviluppo. Di esso fanno parte i Paesi più industrializzati (quelli del G8 *in primis*). In esso è presente, inoltre, l'Unione europea.

Il G20 rappresenta in totale i due terzi del commercio e della popolazione mondiale, oltre all'80% del PIL mondiale. Sono in esso presenti anche alcune tra le maggiori organizzazioni internazionali (Ocse, Fatf, Unodc, World Bank, B20, C20, Y20 etc.).

Dopo il primo incontro nel dicembre 1999 a Berlino, cui parteciparono i Ministri delle Finanze e i Banchieri centrali dei Paesi membri, i successivi *meetings* sono divenuti veri e propri vertici dei Capi di Stato. Il G20 ha difatti progressivamente sostituito il G8 come principale consiglio economico delle nazioni più sviluppate.

I Leader del G20 hanno istituito, all'interno di detto esercizio, il Gruppo di lavoro Anticorruzione (ACWG) in occasione del Summit di Toronto del 2010, per analizzare l'impatto fortemente negativo della corruzione sulla crescita economica, sul commercio e sullo sviluppo.

Il Gruppo si compone di esperti giuridici nazionali espressione del Governo.

Dal 2010 i lavori del Gruppo sono stati dedicati al monitoraggio degli impegni presi da parte dei paesi G20 in merito alla ratifica e implementazione della Convenzione ONU contro la Corruzione, alla

criminalizzazione e investigazione della corruzione in ambito internazionale (*foreign bribery*) e alla cooperazione internazionale per tracciare i proventi della corruzione.

L'ACWG lavora con l'OCSE e la Banca Mondiale per fornire indirizzi di policy ai paesi G20 nella definizione e attuazione delle misure contro la corruzione: nel corso di suddette attività il gruppo di lavoro redige i testi dei documenti recanti *High Level Principles* sulla *governance* anticorruzione mondiale.

Questi documenti vengono adottati dai *Leader* nel *summit* che, di volta in volta, concludono l'esercizio multilaterale ogni anno; essi sono l'espressione della volontà comune di cooperare per il conseguimento dell'obiettivo prescelto.

Con specifico riferimento all'attività anticorruzione, innanzitutto, dal sito del G20 (20.org) è possibile leggere, al punto 16 della dichiarazione ufficiale resa al termine del summit 2015, testualmente: *in support of our growth and resilience agenda, we remain committed to building a global culture of intolerance towards corruption, through effectively implementing the 2015/2016 G20 Anticorruption Action plan. We endorse the High level principles on private sector transparency and security, which will help our companies comply with global standards on ethics and anticorruption Ensuring the integrity and transparency of our public sector is essential. In this regard, we endorse the G20 Anti corruption Open data principles and the G20 principles for promoting integrity in Public Procurement, and we welcome the ongoing work on asset disclosure frameworks. We will further work to strengthen international cooperation, including where appropriate and consistent with domestic legal systems, on civil and administrative procedures, as an important tool to effectively combat bribery and to support asset recovery and the denial of safe haven to corrupt officials and those who corrupt them. We welcome the publication of our implementation plans on beneficial ownership transparency and wil continue our efforts in this regard.*

Gli alti principi in commento iniziano con un ampio preambolo che sottolinea l'essenzialità del settore privato come *partner* nelle politiche anticorruzione; il G20 ha approfondito statisticamente la ricaduta della corruzione domestica e internazionale sul piano della resa dei *business*. Per detti motivi l'integrità nel settore privato rappresenta un'assoluta priorità nelle *policy* mondiali.

Il documento adottato dal Gruppo di lavoro anticorruzione del G20 è destinato ad affiancare le altre linee guida internazionali già vigenti come l'*Anticorruption Ethics and Compliance handbook for Business*, predisposto da UNODC OECD e World Bank oltre al *Anticorruption Ethics and compliance programme for business: a practical guide* di UNODC.

I principi si rivolgono a tutte le imprese, indipendentemente dalle loro dimensioni, e richiamano precedenti documenti pure di rilievo, come *the Guiding principles on enforcement of the foreign bribery offences* (2013), *the guiding principles to combat solicitations* (2013) *the high level principles on beneficial ownership transparency* (2014) e *the G20 principles for promoting integrity in Public Procurement* (2015).

I principi (riportati qui di seguito) percorrono tutta l'attività d'impresa, dal punto di vista organizzativo, della cd. collaborazione attiva, del *risk management*, dell'*audit*, della *compliance*, della *due diligence*.

Principles

The G20 encourages businesses to develop strong, robust and effective internal controls, ethics and compliance programs and/or measures on the basis of a risk assessment to better understand the risk exposure linked to the business's industry, size, legal structure and geographical area of operation, and to allocate resources efficiently and effectively. The following Principles include elements that are important to consider in the development of effective internal controls and ethics and compliance programs, and in promoting transparency and integrity in the private sector. They are intended to be adapted by businesses, in particular SMEs, according to their individual circumstances, including their size, type, legal structure and geographical and industrial sector of operation, as well as the jurisdictional and other basic legal principles under which they operate.

- 1. Businesses should have a clear and accessible policy on prohibiting corruption.*
- 2. Senior management, as well as the board of directors as appropriate, should clearly express and commit to the business's internal controls and ethics and compliance program, good corporate governance, transparency and integrity, for the detection and prevention of corruption. The internal controls and ethics and compliance programs must be enforced at all levels within the business, and senior managers must set the proper tone at the top for employees to follow.*

3. *The board has a key role in setting the ethical tone of a business, not only by its own actions, but also in appointing and overseeing key executives and consequently the management in general.*
4. *Oversight of internal controls and the ethics and compliance program should be the duty of one or more senior corporate officers, endowed with an adequate level of autonomy, resources and independence from management.*
5. *In line with their duties, all individuals within the business should uphold the internal controls and ethics and compliance program, and take responsibility for ensuring the effectiveness of internal controls and the ethics and compliance program.*
6. *Businesses should consider, where appropriate, external communication of their commitment to effective internal controls and ethics and compliance programs.*
7. *The compliance program should be supported by auditing and monitoring of systems of internal accounting controls, which ensure the maintenance of fair and accurate records and detect and prevent corruption.*
8. *Depending on the business's individual circumstances, the internal controls and ethics and compliance program should include appropriately detailed policies and procedures for particular risk areas; such as payments to domestic and foreign public officials, payments to third parties, facilitation payments, gifts, hospitality, entertainment and expenses, travel, political contributions, charitable donations and sponsorships, as well as conflicts of interest, solicitation and extortion.*
9. *Businesses should conduct appropriate due diligence. Due diligence includes vetting new hires, agents, and business partners, and extends to the formation of joint ventures and mergers and acquisitions. Due diligence should be an ongoing process and be commensurate with the associated corruption-related risk factors.*
10. *In cases of mergers and acquisitions, businesses should, as appropriate, promptly incorporate the acquired business into its internal controls and ethics and compliance program.*
11. *Businesses should ensure that their subsidiaries, as well as affiliates over whom they have effective control, have internal controls and ethics and compliance measures commensurate with the risks they face.*

12. *Businesses should take steps to encourage or, according to risk and where appropriate, to ensure that their business partners have effective internal controls and ethics and compliance measures.*
13. *Periodic reviews of the internal controls and the ethics and compliance program should be undertaken to evaluate and improve their effectiveness and take into account evolving standards, business risks, and other circumstances as appropriate.*
14. *Businesses should ensure regular training on their internal controls and ethics and compliance programs.*
15. *Businesses should promote and incentivize observance of their internal controls, and ethics and compliance programs.*
16. *Appropriate corrective and disciplinary action should be taken for failure to comply with internal controls and the ethics and compliance program.*
17. *Effective and easily accessible reporting mechanisms and whistleblower protection should be provided to employees and others who report, on good faith and reasonable grounds, breaches of the law, or violations of the business's policies and procedures. Businesses should undertake appropriate action in response to such reports.*

SOCIETÀ ED ENTI PUBBLICI

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

Aggiornamento 2015 del Piano Nazionale Anticorruzione e decreto 231: ribadite convergenze

La Determina dell'Autorità Nazionale Anticorruzione (ANAC) n. 12, del 28 ottobre 2015 (G.U. n. 267 del 16.11.2015), a oggetto: "Piano Nazionale Anticorruzione - Aggiornamento 2015", ribadisce le convergenze tra Piano triennale di prevenzione della corruzione (PTPC), previsto dalla legge anticorruzione 190 del 2012 (dopo, legge 190) e Modello di organizzazione e gestione, previsto dal decreto legislativo 231 del 2001 (dopo, decreto 231).

Con la Determina n. 8/2015 (Linee guida per l'attuazione della normativa in materia di prevenzione delle 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'ANAC ha precisato, in maniera chiara, i punti d'incontro tra i due corpi normativi (1). Dopo aver ribadito l'obbligo delle amministrazioni pubbliche che controllano società o vi partecipano di promuovere, presso questi soggetti, l'adozione del Modello di organizzazione e gestione previsto del decreto 231, sostanzialmente suggerisce che, se il Modello è stato adottato, sia opportunamente integrato con misure idonee a prevenire anche i fenomeni di corruzione e di illegalità in coerenza con le finalità della legge 190. Ciò poiché il concetto di corruzione presente nella legge 190 è più ampio della definizione del fenomeno contenuta nel reato di corruzione previsto dall'ordinamento penale, cui fa riferimento il decreto 231. Per la legge 190, infatti, la corruzione comprende anche tutti i fatti di "maladministration", intesa come assunzione di decisioni devianti dalla cura dell'interesse generale a causa del comportamento improprio da parte di interessi particolari. In altre parole, come "adozione di comportamenti e atti contrari,

(1) Ampiamente in punto, MANACORDA, Società ed enti controllati e partecipati da pubbliche amministrazioni e norme anticorruzione: il ruolo del decreto 231 nell'interpretazione dell'Autorità nazionale anticorruzione e del Ministero dell'economia e delle finanze, in La responsabilità amministrativa delle società e degli enti, 3/2015, 217 ss.

più in generale, al principio di imparzialità cui sono tenuti tutte le p.a. e i soggetti che svolgono attività di pubblico interesse”.

Con il nuovo provvedimento l'ANAC, dopo aver richiamato le direttive già diffuse con la precitata Determina n. 8/2015 circa le modalità applicative della legge 190 alle società controllate o partecipate dalla pubblica amministrazione, agli enti di diritto privato in controllo pubblico e agli enti pubblici economici, puntualizza che: “Ai fini della completezza dell'analisi organizzativa dei processi/procedimenti e della individuazione delle misure di prevenzione, a tali soggetti si applicano le disposizioni del presente Aggiornamento”. Ribadisce tuttavia che, ove la partecipazione della pubblica amministrazione sia in società ed in altri enti di diritto privato, “l'adozione di misure integrative di quelle del decreto legislativo 231/2001 è promossa dalle amministrazioni partecipanti”.

Ciò premesso, merita richiamare, brevemente, alcuni punti qualificanti della Determina dell'ANAC n. 12.

L'Autorità precisa, preliminarmente, che l'Aggiornamento del Piano nazionale anticorruzione – approvato con delibera n. 72 del 2013 – si rende necessario, essenzialmente, per:

- offrire un supporto operativo che consenta alle pubbliche amministrazioni e agli altri soggetti tenuti all'introduzione di misure di prevenzione della corruzione di apportare eventuali correzioni volte a migliorare l'efficacia complessiva dell'impianto anticorruzione adottato(2);
- dare risposte unitarie alle richieste di chiarimenti pervenute dagli operatori;
- adeguare le linee precedenti alla luce degli interventi normativi frattanto intervenuti riguardanti il sistema di prevenzione della corruzione. Segnatamente: decreto-legge 90/2014, convertito nella legge 114/2014 (art. 19), che sopprime l'Autorità per la vigilanza sui contratti pubblici e ne trasferisce le funzioni all'ANAC (cc. 1 e 2), e trasferisce dal Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei

(2) L'Autorità riferisce di aver svolto un monitoraggio sulla qualità dei PTPC di un campione di 1911 amministrazioni e di averli trovati generalmente insoddisfacenti per: insufficienza e inadeguatezza - se non addirittura assenza - dell'analisi del contesto esterno; bassa qualità e scarsa analiticità della mappatura dei processi; insufficiente mappatura e trattamento del rischio; assenza di un efficace coordinamento tra PTPC e Piano della performance; criticità nel coinvolgimento di soggetti interni ed esterni; insufficiente monitoraggio interno dei PTPC.

Ministri all'ANAC tutte le competenze sulla prevenzione della corruzione e sulla trasparenza (c. 15).

L'Autorità fornisce quindi alcune indicazioni metodologiche per la redazione e il miglioramento dei PTPC con riguardo a:

- analisi del contesto interno ed esterno;
- mappatura dei processi;
- valutazione del rischio;
- trattamento del rischio;
- monitoraggio del PTPC.

Il provvedimento dell'ANAC, dopo aver osservato di aver “ritenuto opportuno fornire alcune esemplificazioni di eventi corruttivi e relative misure con riferimento all'area di rischio contratti pubblici e al settore della Sanità”, dedica ai due argomenti una “Parte speciale”. La parte speciale dedicata al settore della Sanità riguarda, ovviamente, le problematiche proprie di esso. Più ampia applicazione hanno, invece, le indicazioni e gli approfondimenti riguardanti la predisposizione e la gestione delle misure di prevenzione della corruzione nell'area di rischio relativa ai contratti pubblici di lavori, servizi e forniture. Come noto, è infatti in questo settore che possono manifestarsi diffuse situazioni di corruzione, segnatamente nell'ampia accezione del termine che le gli assegna l'Autorità.

Benché la Determina n 12 non ne faccia menzione, per l'applicazione delle direttive ANAC nel settore dei contratti pubblici occorrerà verificare se si applichino all'ente che deve operare le norme del Codice dei contratti pubblici di lavori, servizi e forniture, di cui al decreto legislativo 163 del 2006. Viene qui in causa il concetto di “organismo di diritto pubblico”, quale definito al punto 26 dell'articolo 3 del Codice, e se tale qualificazione sia attribuibile a tutte le amministrazioni pubbliche e alle società controllate e partecipate dalla pubblica amministrazione.

Una *road map* degli adempimenti 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 è stata ridefinita con Comunicato del Presidente dell'ANAC del 25 novembre 2015.