

Premessa

Per disporre di un quadro completo e chiaro della disciplina penalistica cui il D.Lgs. n. 231 del 2001 si riferisce nel prevedere la responsabilità amministrativa dell'ente dipendente dal reato commesso da chi agisce (soggetto di vertice o subordinato) nell'interesse od a vantaggio dell'ente stesso, è utile riportare qui di seguito il contenuto delle singole norme rilevanti. Per ciascuna di esse, o per gruppi omogenei, sono richiamate le macroattività tipiche dei processi organizzativi, onde fornire un diretto ed immediato collegamento tra i singoli reati dai quali può discendere la responsabilità dell'ente ed i settori aziendali sensibili, nel cui ambito possono verificarsi comportamenti illeciti che il sistema di controllo mira a prevenire.

Ciò anche al fine di favorire - attraverso una diffusa azione di informazione e formazione aziendale - la conoscenza dei rischi in rapporto al ruolo rivestito dal singolo all'interno dell'organizzazione aziendale e comprendere la ratio delle specifiche prescrizioni dettate nel Modello.

Le famiglie di reati per le quali il Dlgs 231/2001 e s.m.i. prevede la responsabilità amministrativa dell'ente sono le seguenti:

Art. 24	<p>Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico</p> <ul style="list-style-type: none"> ▪ Malversazione a danno dello Stato (art. 316-bis c.p.) ▪ Indebita percezione di erogazioni a danno dello Stato (art.316-ter c.p.) ▪ Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.) ▪ Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bisc.p.) ▪ Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.) 	
Art. 24-bis	<p>Delitti informatici e trattamento illecito di dati</p> <ul style="list-style-type: none"> ▪ Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.) ▪ Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) ▪ Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.) ▪ Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.) ▪ Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617- quater c.p.) ▪ Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) ▪ Danneggiamento di informazioni, dati e programmi informatici (art. 635-bisc.p.) ▪ Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) ▪ Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) ▪ Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635- quinquies c.p.) ▪ Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.) 	aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016
Art. 24-ter	Delitti di criminalità organizzata	aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 2 di 85
------------------------------	---------------------	-----------------	-------------------

	<ul style="list-style-type: none"> ▪ Associazione per delinquere (art. 416 c.p.) ▪ Associazione di tipo mafioso anche straniere (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015] ▪ Scambio elettorale politico-mafioso (art. 416-ter c.p.) ▪ Sequestro di persona a scopo di estorsione (art. 630 c.p.) ▪ Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309) ▪ Tutti i delitti se commessi avvalendosi delle condizioni previste dall'art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91) ▪ Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, co. 2, lett. a), numero 5), c.p.p.) 	
Art. 25	<p>Concussione, induzione indebita a dare o promettere altra utilità e corruzione</p> <ul style="list-style-type: none"> ▪ Concussione (art. 317 c.p.) [articolo modificato dalla L. n. 69/2015] ▪ Corruzione per l'esercizio della funzione (art. 318 c.p.) [articolo modificato dalla L. n. 190/2012 e L. n. 69/2015] ▪ Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [articolo modificato dalla L. n. 69/2015] ▪ Circostanze aggravanti (art. 319-bis c.p.) ▪ Corruzione in atti giudiziari (art. 319-ter c.p.) [articolo modificato dalla L. n. 69/2015] ▪ Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015] ▪ Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.) ▪ Pene per il corruttore (art. 321 c.p.) ▪ Istigazione alla corruzione (art. 322 c.p.) ▪ Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) [articolo modificato dalla L. n. 190/2012] 	<p>modificato dalla L. n. 190/2012</p>
Art. 25-bis	<p>Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento</p>	<p>aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs. 125/2016</p>

	<ul style="list-style-type: none"> ▪ Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.) ▪ Alterazione di monete (art. 454 c.p.) ▪ Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.) ▪ Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.) ▪ Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.) ▪ Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.) ▪ Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.) ▪ Uso di valori di bollo contraffatti o alterati (art. 464 c.p.) ▪ Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.) ▪ Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.) 	
Art. 25-bis.1	<p>Delitti contro l'industria e il commercio</p>	aggiunto dalla L. n. 99/2009
	<ul style="list-style-type: none"> ▪ Turbata libertà dell'industria o del commercio (art. 513 c.p.) ▪ Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.) ▪ Frodi contro le industrie nazionali (art. 514 c.p.) ▪ Frode nell'esercizio del commercio (art. 515 c.p.) ▪ Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.) ▪ Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) ▪ Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.) ▪ Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.) 	
Art. 25-ter	<p>Reati societari</p>	aggiunto dal D.Lgs. n. 61/2002; modificato dalla L. n. 190/2012, dalla L. 69/2015 e dal D.Lgs. n. 38/2017
	<ul style="list-style-type: none"> ▪ False comunicazioni sociali (art. 2621 c.c.) [articolo modificato dalla L. n. 69/2015] ▪ Fatti di lieve entità (art. 2621-bis c.c.) ▪ False comunicazioni sociali delle società quotate (art. 2622 c.c.) [articolo modificato dalla L. n. 69/2015] ▪ Impedito controllo (art. 2625, comma 2, c.c.) ▪ Indebita restituzione di conferimenti (art. 2626 c.c.) ▪ Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.) ▪ Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) ▪ Operazioni in pregiudizio dei creditori (art. 2629 c.c.) ▪ Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla legge n. 262/2005] ▪ Formazione fittizia del capitale (art. 2632 c.c.) ▪ Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) ▪ Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla legge n. 190/2012; articolo modificato dal D.Lgs. n. 38/2017] ▪ Istigazione alla corruzione tra privati (art. 2635-bis c.c.) [aggiunto dal D.Lgs. n. 38/2017] ▪ Illecita influenza sull'assemblea (art. 2636 c.c.) ▪ Aggiotaggio (art. 2637 c.c.) ▪ Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.) 	

Art. 25- quater	Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali	aggiunto dalla L. n. 7/2003
	<ul style="list-style-type: none"> ▪ Associazioni sovversive (art. 270 c.p.) ▪ Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.) ▪ Assistenza agli associati (art. 270 ter c.p.) ▪ Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.) ▪ Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.) ▪ Finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270 quinquies.1 c.p.) ▪ sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.) ▪ Condotte con finalità di terrorismo (art. 270 sexies c.p.) ▪ Attentato per finalità terroristiche o di eversione (art. 280 c.p.) ▪ Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.) ▪ Atti di terrorismo nucleare (art. 280 ter c.p.) ▪ Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.) ▪ Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.) ▪ Cospirazione politica mediante accordo (art. 304 c.p.) ▪ Cospirazione politica mediante associazione (art. 305 c.p.) ▪ Banda armata: formazione e partecipazione (art. 306 c.p.) ▪ Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.) ▪ Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1) ▪ Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2) ▪ Sanzioni (L. n. 422/1989, art. 3) ▪ Pentimento operoso (D.Lgs. n. 625/1979, art. 5) ▪ Convenzione di New York del 9 dicembre 1999 (art. 2) 	
Art. 25- quater.1	Pratiche di mutilazione degli organi genitali femminili	aggiunto dalla L. n. 7/2006
	<ul style="list-style-type: none"> ▪ Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.) 	
Art. 25- quinquies	Delitti contro la personalità individuale	aggiunto dalla L. n. 228/2003 e modificato dalla L. n. 199/2016
	<ul style="list-style-type: none"> ▪ Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.) ▪ Prostituzione minorile (art. 600-bis c.p.) ▪ Pornografia minorile (art. 600-ter c.p.) ▪ Detenzione di materiale pornografico (art. 600-quater) ▪ Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38] ▪ Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.) ▪ Tratta di persone (art. 601 c.p.) ▪ Acquisto e alienazione di schiavi (art. 602 c.p.) ▪ Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.) ▪ Adescamento di minorenni (art. 609-undecies c.p.) 	

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 5 di 85
------------------------------	---------------------	-----------------	-------------------

Art. 25- sexies	Reati di abuso di mercato	aggiunto dalla L. n. 62/2005
	<ul style="list-style-type: none"> ▪ Abuso di informazioni privilegiate (art. 184 D. Lgs. n.58/1998) ▪ Manipolazione del mercato (art. 185 D. Lgs. n. 58/1998) 	
Art. 25- septies	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinforturistiche e sulla tutela dell'igiene e della salute sul lavoro	aggiunto dalla L. n. 123/2007
	<ul style="list-style-type: none"> ▪ Omicidio colposo (art. 589 c.p.) ▪ Lesioni personali colpose (art. 590 c.p.) 	
Art. 25- octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014
	<ul style="list-style-type: none"> ▪ Ricettazione (art. 648 c.p.) ▪ Riciclaggio (art. 648-bis c.p.) ▪ Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) ▪ Autoriciclaggio (art. 648-ter.1 c.p.) 	

Art. 25- novies	Delitti in materia di violazione del diritto d'autore	aggiunto dalla L. n. 99/2009
	<ul style="list-style-type: none"> ▪ Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis) ▪ Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3) ▪ Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1) ▪ Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2) ▪ Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941) ▪ Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941) ▪ Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941) 	
Art. 25- decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	aggiunto dalla L. n. 116/2009
	<ul style="list-style-type: none"> ▪ Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) 	
Art. 25- undecies	Reati ambientali	aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 7 di 85
------------------------------	---------------------	-----------------	-------------------

	<ul style="list-style-type: none"> ▪ Inquinamento ambientale (art. 452-bis c.p.) ▪ Disastro ambientale (art. 452-quater c.p.) ▪ Delitti colposi contro l'ambiente (art. 452-quinquies c.p.) ▪ Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.) ▪ Circostanze aggravanti (art. 452-octies c.p.) ▪ Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.) ▪ Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733- bis c.p.) ▪ Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6) ▪ Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D. Lgs n.152/2006, art. 137) ▪ Attività di gestione di rifiuti non autorizzata (D. Lgs n.152/2006, art.256) ▪ Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D. Lgs n. 152/2006, art. 257) ▪ Traffico illecito di rifiuti (D. Lgs n.152/2006, art. 259) ▪ Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D. Lgs n.152/2006, art. 258) ▪ Attività organizzate per il traffico illecito di rifiuti (D. Lgs n.152/2006, art. 260) ▪ False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D. Lgs n.152/2006, art. 260-bis) ▪ Sanzioni (D.Lgs. n. 152/2006, art. 279) ▪ Inquinamento doloso provocato da navi (D. Lgs. n.202/2007, art.8) ▪ Inquinamento colposo provocato da navi (D. Lgs. n.202/2007, art.9) 	
Art. 25- duodecies	<p>Impiego di cittadini di paesi terzi il cui soggiorno è irregolare</p> <ul style="list-style-type: none"> ▪ Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.Lgs. n. 286/1998) 	aggiunto dal D.Lgs. n. 109/2012
Art. 12, L. n. 9/2013	<p>Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato <i>[Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva]</i></p> <ul style="list-style-type: none"> ▪ Impiego Adulterazione e contraffazione di sostanze alimentari (art. 440 c.p.) ▪ Commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.) ▪ Commercio di sostanze alimentari nocive (art. 444 c.p.) ▪ Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 c.p.) ▪ Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.) ▪ Frode nell'esercizio del commercio (art. 515 c.p.) ▪ Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.) ▪ Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) ▪ Contraffazione di indicazioni geografiche denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.) 	

L. n. 146/2006	Reati transnazionali [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]	
	<ul style="list-style-type: none">▪ Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D. Lgs. 25 luglio 1998, n. 286)▪ Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)▪ Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)▪ Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)▪ Favoreggiamento personale (art. 378 c.p.)▪ Associazione per delinquere (art. 416 c.p.)▪ Associazione di tipo mafioso (art. 416-bis c.p.)	

Art. 24 d.lgs. 231/2001 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico

Reati presupposto		
Codice penale	art. 316 <i>bis</i>	Malversazione a danno dello Stato
	art. 316 <i>ter</i>	Indebita percezione di erogazioni a danno dello Stato
	art. 640	Truffa aggravata a danno dello Stato
	art. 640 <i>bis</i>	Truffa aggravata per il conseguimento di erogazioni pubbliche
	art. 640 <i>ter</i>	Frode informatica

1. CONSIDERAZIONI GENERALI

Il delitto di truffa aggravata in danno dello Stato è realizzabile in tutti gli ambiti aziendali che prevedono rapporti o contatti con la PA. La truffa si caratterizza per l'immutazione del vero in ordine a situazioni la cui esistenza, nei termini falsamente rappresentati, è essenziale per l'atto di disposizione patrimoniale da parte della P.A.

La frode informatica, invece, assume rilievo ai fini della responsabilità dell'ente solo se realizzata in danno della P.A. Il reato di frode informatica presenta, sostanzialmente, la medesima struttura e i medesimi elementi costitutivi del reato di truffa da cui si distingue in quanto l'attività illecita investe non la persona ma un sistema informatico. Nel reato di frode informatica, pertanto, non assume rilevanza - a differenza che nel reato di truffa - il ricorso da parte dell'autore del reato ad artifici o raggiri, ma l'elemento oggettivo dell'alterazione del sistema informatico (e/o dei dati in esso disponibili). Si tratta di una tipologia di illecito oggi poco frequente ma che, è prevedibile, avrà nel futuro più ampia realizzazione. Al contrario, i reati in materia di erogazioni pubbliche (art. 316 *bis*, 316 *ter* e 640 *bis* c.p.) sono piuttosto ricorrenti, soprattutto in certe aree geografiche.

Le fattispecie da ultimo richiamate mirano a tutelare l'erogazione di finanziamenti pubblici, comunque denominate, sotto due diversi profili temporali: nel momento di erogazione e nel successivo momento dell'utilizzazione dei finanziamenti. Le condotte punite, con riferimento al primo dei due momenti, sono modellate sullo schema della truffa in cui assume rilevanza determinante l'immutazione del vero in ordine ad aspetti essenziali ai fini dell'erogazione. Nella malversazione, invece, assume rilievo la mancata destinazione del finanziamento ricevuto per le finalità di interesse pubblico che ne abbiano giustificato l'erogazione.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Aree a rischio reato	Controlli preventivi
<p>Partecipazione ad una gara indetta da un soggetto pubblico, ovvero presentazione di istanze alla P.A. al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc) di interesse aziendale (ad es. mediante la produzione di documenti falsi attestanti l'esistenza di condizioni e/o requisiti essenziali).</p>	<p>Specifiche previsioni nel sistema aziendale di programmazione e di controllo.</p> <p>Puntuali attività di controllo gerarchico (incluso sistema di deleghe).</p>
<p>Attività aziendali che prevedano l'accesso nei confronti di sistemi informativi gestiti dalla PA, quali, a titolo esemplificativo: la partecipazione a procedure di gara che prevedono comunque una gestione informatica (ad es. mediante l'alterazione di registri informatici della PA per far risultare esistenti condizioni essenziali per la partecipazione: iscrizione in albi, ecc.); la presentazione in via informatica alla P.A. di istanze e documentazione di supporto, al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc) di interesse aziendale (ad es. laddove contenenti attestazioni/certificazioni non veritiere in merito all'esistenza di condizioni e/o requisiti essenziali); i rapporti con soggetti della P.A. competenti in materia fiscale o previdenziale in relazione alla ipotesi di</p>	<p>Sistema di controlli interno all'azienda che, ai fini del corretto e legittimo accesso ai Sistemi informativi della PA, preveda:</p> <ul style="list-style-type: none"> • un adeguato riscontro delle <i>password</i> di abilitazione per l'accesso ai Sistemi Informativi della PA possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche funzioni/strutture aziendali; • la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dalla società; • il rispetto della normativa sulla <i>privacy</i>. <p>Questi meccanismi assumono maggiore pregnanza per quelle società o enti che, sulla base di un rapporto di appalto/concessione con una PA o in qualità di società miste partecipate da un'Amministrazione/Ente locale e da un privato imprenditore, si assumono l'incarico di realizzare, sviluppare e gestire un Sistema Informativo pubblico o un Sistema Informativo di interesse pubblico.</p>

<p>modifica in via informatica dei dati (es. fiscali e/o previdenziali) di interesse dell'azienda (es. modelli 770), già trasmessi alla P.A.</p>	
<p>Le aree maggiormente a rischio sono relative a:</p> <ul style="list-style-type: none"> • settore delle attività finanziarie; • investimenti ambientali; • investimenti di produzione; • ricerca ed innovazione tecnologica. 	<p>Specifica previsione del codice etico e diffusione di quest'ultimo tra tutti i dipendenti.</p> <p>Programma di informazione/formazione periodica del dipendente. Responsabilizzazione esplicita, riportata in ordine di servizio e nel contesto delle relative procedure aziendali, delle funzioni competenti alla predisposizione dei progetti e delle relative istanze.</p> <p>Separazione funzionale fra chi gestisce le attività di realizzazione e chi presenta la documentazione di avanzamento.</p> <p>Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto).</p> <p>Coerenza delle procure verso l'esterno con il sistema delle deleghe. Esclusione esplicita, nel sistema delle procure, della "richiesta di denaro o altra utilità a terzi".</p> <p>Puntuali attività di controllo gerarchico, previste altresì in sede di Ordine di servizio delle Funzioni competenti che partecipano al processo di acquisizione di beni e servizi per la società.</p>
<p>Partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego.</p> <p>In tale contesto, assumono particolare rilevanza i seguenti ambiti di operatività:</p> <ul style="list-style-type: none"> • formazione; • ricerca ed innovazione tecnologica; • investimenti ambientali; • gestione delle attività finanziarie; • investimenti di produzione. 	<p>Controlli di completezza e correttezza della documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto).</p> <p>Verifiche incrociate di coerenza tra la funzione richiedente l'erogazione pubblica e la funzione designata a gestire le risorse per la realizzazione dell'iniziativa dichiarata.</p> <p>Monitoraggio sull'avanzamento del progetto realizzativo (a seguito dell'ottenimento del contributo pubblico) e sul relativo <i>reporting</i> alla PA, con evidenza e gestione delle eventuali anomalie.</p> <p>Controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.</p>

Art. 24-bis d.lgs. 231/2001 - Delitti informatici e trattamento illecito di dati

Reati presupposto		
Codice penale	art. 491 bis	Falsità riguardanti un documento informatico
	art. 615 ter	Accesso abusivo ad un sistema informatico o telematico
	art. 615 quater	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici
	art. 615 quinquies	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
	art. 617 quater	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
	art. 617 quinquies	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
	art. 635 bis	Danneggiamento di informazioni, dati e programmi informatici
	art. 635 ter	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
	art. 635 quater	Danneggiamento di sistemi informatici o telematici
	art. 635 quinquies	Danneggiamento di sistemi informatici o telematici di pubblica utilità
	art. 640 quinquies	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

1. CONSIDERAZIONI

L'articolo 24-bis del decreto 231 ha esteso la responsabilità amministrativa delle persone giuridiche e degli enti alla quasi totalità dei reati informatici.

Alla luce dei presupposti applicativi del decreto, gli enti saranno considerati responsabili per i delitti informatici commessi nel loro interesse o a loro vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa, ma anche da persone sottoposte alla loro direzione o vigilanza. Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri, obiettivo stesso della condotta e, in altri, lo strumento attraverso cui l'autore intende realizzare altra fattispecie penalmente rilevante.

Lo sviluppo della tecnologia informatica ha generato nel corso degli anni modifiche sostanziali nell'organizzazione del *business* di impresa e ha inciso sensibilmente sulle opportunità a disposizione di ciascun esponente aziendale per realizzare o occultare non soltanto schemi di condotte criminali già esistenti ma anche fattispecie nuove, tipiche del cd. mondo virtuale.

A ciò si aggiunge l'ingresso massivo di dispositivi mobili (es. *tablet* e *smartphone*), l'utilizzo di server di *cloud computing* (per esempio servizi di memorizzazione e archiviazione dei dati distribuiti su reti e *server* remoti) che:

moltiplicano le opportunità di realizzazione di un reato informatico;

introducono criticità in relazione al loro utilizzo aziendale in virtù dei ridotti interventi del legislatore italiano e- soprattutto - della carenza di convenzioni internazionali che si renderebbero ancor più necessarie in virtù della globalità del fenomeno;

determinano la necessità per le imprese di adeguarsi rapidamente al fine di disciplinare correttamente la gestione di tali fenomeni.

Quanto ai soggetti maggiormente esposti a tale fattispecie di reato, tale fenomeno può potenzialmente coinvolgere qualsiasi ente che utilizzi in maniera rilevante gli strumenti informatici e telematici per lo svolgimento delle proprie attività. È chiaro, tuttavia, che tale categoria di reato risulta di più probabile accadimento in quei settori attivi nell'erogazione di servizi legati *all'Information Technology* (es. gestione delle infrastrutture di rete, sistemi di e-commerce, etc.) ovvero in cui tali servizi costituiscono un valore aggiunto per il cliente (es. soluzioni di e-commerce, gestione di pagamenti *on line*, etc.).

Con riguardo alle aree aziendali più esposte al rischio di commissione di tale categoria di reato presupposto, è bene evidenziare che l'accesso alla tecnologia ha fortemente dilatato il perimetro dei potenziali autori di condotte delittuose, sebbene vi siano aree aziendali (es. area amministrazione, finanza e controllo, marketing, area R&S, area ICT, area acquisti e appalti) che risultano maggiormente esposte al rischio di commissione di reati informatici che possano determinare un interesse o un vantaggio economico per l'azienda¹.

Le imprese dovranno anche verificare che il loro stato in tema di ICT *Security Governance & Management* sia tale da aspirare al riconoscimento dell'esimente dalla responsabilità prevista dal decreto 231 in caso di commissione di un delitto informatico al loro interno. In altri termini, si tratterà di verificare l'esistenza di misure di sicurezza preventive e di controllo idonee a evitare la commissione dei reati informatici e provvedere all'adeguamento dei propri modelli di organizzazione, gestione e controllo, laddove necessario.

La prevenzione dei crimini informatici deve essere svolta attraverso adeguate misure organizzative, tecnologiche e normative, assicurando che l'attività dell'Organismo di Vigilanza venga indirizzata anche verso specifiche forme di controllo degli aspetti sintomatici di anomalie del sistema informativo, in linea con quanto previsto dalle Linee Guida su compiti e poteri dell'Organismo di Vigilanza. Dovrebbero quindi essere previsti almeno i seguenti **controlli di carattere generale**:

previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno dell'ente, che tramite apparecchiature non soggette al controllo dello stesso;

¹ Proprio in considerazione della trasversalità del rischio di commissione dei reati di cui all'articolo 24 *bis* del decreto 231 rispetto alle aree aziendali, lo schema di cui al successivo punto 2 enuclea potenziali modalità di commissione dell'illecito piuttosto che le aree a rischio reato.

previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali forniti;

predisposizione di adeguati strumenti tecnologici (es. *software*) atti a prevenire e/o impedire la realizzazione di illeciti informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture aziendali ritenute più esposte al rischio;

predisposizione di programmi di informazione, formazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

previsione di idonee clausole nei contratti conclusi con i *provider* di servizi legati all'*Information Technology*. A ciò si aggiunga la

necessità - in virtù dei recenti sviluppi tecnologici - di adottare *policy* e procedure organizzative concernenti:

l'utilizzo di apparecchi personali sul luogo di lavoro (cd. *BYOD policy*), qualora ammessi, che prevedano, a titolo esemplificativo: *i*) la regolamentazione dell'uso dei suddetti apparecchi (quali *tablet* e *smartphone*) a fini lavorativi; *ii*) la selezione e definizione di *browser*, programmi, *social network* e applicazioni il cui uso è permesso/tollerato/limitato/vietato all'interno del contesto aziendale; *iii*) l'adozione di sistemi di *logging* e di *monitoring* nei limiti consentiti; *iv*) la previsione di un sistema interno di gestione degli apparecchi, comprendente la programmazione degli stessi e l'assistenza tecnica; *v*) l'adozione di azioni di cancellazione di dati e bloccaggio in remoto dei dispositivi;

l'utilizzo di sistemi di cd. *cloud computing* che prevedano, a titolo esemplificativo: *i*) la scelta dei cd. *cloud server* ammessi dall'azienda sulla base di criteri stabiliti da *policy* interne (es. affidabilità del gestore, accessibilità del servizio, ecc.); *ii*) la regolamentazione e/o restrizione dell'uso di servizi di *clouding* per il salvataggio e la trasmissione di determinate tipologie di documenti aziendali; *iii*) la definizione e diffusione di linee guida per l'utilizzo dei servizi di *clouding* da parte di tutti gli esponenti dell'azienda.

Il sistema di controllo per la prevenzione dei reati di criminalità informatica dovrà altresì basarsi, ove applicabili, sui seguenti **principi di controllo**:

separazione dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio; tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio; procedure e livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio; raccolta, analisi e gestione di segnalazioni di fattispecie a rischio di reati informatici rilevati da soggetti interni e esterni all'ente;

procedure di *escalation* per la gestione di fattispecie a rischio di reato caratterizzate da elevata criticità e nella gestione dei rapporti con gli enti istituzionali.

L'ambito di applicazione dell'articolo 24-bis è tale da richiedere competenze tecniche ed esperienze specifiche ai fini dello svolgimento delle attività necessarie per la *compliance* al decreto 231: definizione delle possibili modalità di realizzazione dei reati, valutazione dei relativi rischi connessi alle carenze del sistema informatico, valutazione dell'efficacia dei presidi esistenti e definizione delle azioni correttive/integrative.

In ossequio a quanto già previsto nella parte generale delle presenti Linee Guida, con riferimento a questa categoria di reati - più che ad altre - si ritiene particolarmente consigliabile al fine di un efficace controllo preventivo un supporto dell'Organismo di Vigilanza da parte di soggetti in possesso di conoscenze tecniche specifiche (funzioni aziendali interne IT o consulenti esterni).

Si sottolinea che il rispetto di *framework* e *standard* internazionalmente riconosciuti in tema di ICT Security Governance, Management & Compliance, rappresenta un elemento qualificante ai fini della predisposizione di possibili presidi e dell'implementazione di un adeguato sistema di controllo. Riferimenti utili possono essere, tra gli altri:

COBIT (*Control Objectives for Information and related Technology*);

ISO 27001:2005 (norma internazionale che fornisce i requisiti per un sistema di gestione della sicurezza)².

Allo stesso modo è utile richiamare il rispetto di leggi e regolamenti applicabili alla materia della protezione e della sicurezza di dati personali e sistemi informatici (Codice in materia di protezione dei dati personali - decreto n. 196 del 2003 - provvedimenti del Garante Privacy, regolamenti e procedure sugli abusi di mercato, artt. 4 e 8 della legge n. 300 del 1970, ecc.).

2. MODALITÀ DI REALIZZAZIONE DEL REATO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Come accennato nelle considerazioni generali, le specifiche misure di controllo preventivo indicate in tabella sono riprese dallo standard ISO 27001:2005, di cui in parentesi è riportata la numerazione.

Modalità di realizzazione del reato	Controlli preventivi
<p>Art. 491 bis c.p. Falsificazione di documenti informatici da parte di enti che procedono a rendicontazione elettronica di attività. Cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi, allo scopo di eliminare le prove di un altro reato (es. l'ente ha ricevuto un avviso di garanzia per un reato e procede ad eliminare le tracce elettroniche del reato stesso).</p>	<p>Misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate (A.10.9.3); Misure di protezione dei documenti elettronici (es. firma digitale) (A.12.3.1); Procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali (A.15.1.2).</p>

² A tali requisiti si farà riferimento nel seguito, trattando le modalità realizzative e i controlli preventivi relativi ai singoli reati.

Confindustria

<p>Falsificazione di documenti informatici contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti tra privati e PA (es. riduzione degli importi) o alterazione dei documenti in transito nell'ambito del SIPA (Sistema Informatizzato pagamenti della PA) al fine di aumentare gli importi dovuti dalla PA all'ente.</p> <p>Falsificazione di documenti informatici compiuta nell'ambito dei servizi di <i>Certification Authority</i> da parte di un soggetto che rilasci certificati informatici, aventi valenza probatoria, corrispondenti a false identità o attestanti falsi titoli professionali.</p> <p>Falsificazione di documenti informatici correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che queste risultino eseguite dai soggetti legittimi titolari dei dati (es. attivazione di servizi non richiesti).</p>	
<p>Art. 615-ter c.p. Violazione dei sistemi informatici dei concorrenti per acquisire a scopo di spionaggio industriale la documentazione relativa ai loro prodotti/progetti. Tale condotta assume particolare rilievo per gli enti la cui attività è basata su brevetti/disegni/attività di R&S (es. <i>automotive, design, moda, tecnologie, ecc.</i>).</p> <p>Accesso abusivo a sistemi informatici di concorrenti allo scopo di acquisire informazioni concernenti la clientela utili per esempio per l'elaborazione di strategie di <i>marketing</i> (es. dati di consumo, aree geografiche di riferimento,</p>	<p>L'accesso abusivo, oltre ad essere di per sé un illecito, può essere strumentale alla realizzazione di altre fattispecie criminose. I controlli predisposti per prevenire tale fattispecie di reato potrebbero pertanto risultare efficaci anche per la prevenzione di altri reati. Tra tali controlli si segnalano:</p> <ul style="list-style-type: none"> • adozione di procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche; • procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (A.8.3.3 e A.11.2.1); • aggiornamento regolare dei sistemi informativi in uso; • modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo

<p>banche dati, etc.).</p> <p>Accesso abusivo a sistemi di enti pubblici per l'acquisizione di informazioni riservate (es. amministrazione giudiziaria o finanziaria).</p> <p>Accesso abusivo a sistemi interbancari al fine di modificare le informazioni sul proprio conto registrate su tali sistemi.</p> <p>Accesso abusivo a sistemi aziendali protetti da misure di sicurezza, per attivare servizi non richiesti dalla clientela.</p> <p>Accesso abusivo ai sistemi che realizzano la fatturazione dei servizi ai clienti per alterare le informazioni e i programmi al fine di realizzare un profitto illecito.</p> <p>Accesso abusivo ai sistemi che elaborano le buste paghe per alterare i dati relativi alle voci di cedolino al fine di ridurre illecitamente le erogazioni nei confronti degli stessi e realizzare così un interesse o un vantaggio per l'ente.</p> <p>Accesso abusivo ai sistemi che gestiscono il credito di clienti di servizi pre-pagati per modificare i dati di credito e realizzare un profitto per l'ente (come ad esempio avviene nei settori delle telecomunicazioni).</p>	<p>ricoperto dal soggetto (A.11.2.2, A.11.5.1 e A.11.5.2);</p> <ul style="list-style-type: none"> • procedura per il controllo degli accessi (A.11.1.1); • tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali (A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.2); • definizione e attuazione di un processo di autorizzazione della direzione per le strutture di elaborazione delle informazioni (A.6.1.4).
<p>Art. 615-quater c.p.</p> <p>Detenzione e utilizzo di <i>password</i> di accesso a siti di enti concorrenti al fine di acquisire informazioni riservate.</p> <p>Detenzione ed utilizzo di <i>password</i> di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse</p>	<p>Inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni (A.6.1.5).</p> <p>Procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (A.8.3.3 e A.11.2.1).</p>

dell'azienda, anche in violazione di leggi sulla *privacy* o dello statuto dei lavoratori.
 Detenzione abusiva di codici di accesso a sistemi informatici dell'amministrazione giudiziaria o finanziaria al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano l'azienda.
 Diffusione abusiva di numeri seriali di telefoni cellulari altrui al fine della clonazione degli apparecchi.

Art. 617-quater e 617-quinquies c.p.

Intercettazione fraudolenta di comunicazioni di enti concorrenti nella partecipazione a gare di appalto o di fornitura svolte su base elettronica (*e-marketplace*) per conoscere l'entità dell'offerta del concorrente. Tale tipologia di gestione degli acquisti/gare è frequente nell'ambito della PA.

Impedimento o interruzione di una comunicazione al fine di evitare che un concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.

Intercettazione fraudolenta di una comunicazione tra più parti al fine di veicolare informazioni false o comunque alterate, ad esempio per danneggiare l'immagine di un concorrente

Intercettazione delle comunicazioni telematiche della clientela al fine di analizzarne le abitudini di consumo

Impedimento del regolare funzionamento di apparecchi deputati al controllo delle emissioni

Definizione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3).
 Elaborazione di procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione (A.7.2.2);
 Utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse (A.9.1.1).
 Allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione (A.9.2.5 e A.10.8.3).
 Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato (A.10.1.1 e A.10.1.2).
 Previsione di controlli su: rete aziendale e informazioni che vi transitano (A.10.6.1);
 instradamento (*routing*) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza (A.11.4.7);
 installazione di *software* sui sistemi operativi (A.12.4.1).
 Predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).

prodotte da impianti, ad esempio al fine di occultare il superamento dei limiti consentiti e, conseguentemente, la revoca di autorizzazioni amministrative

Installazione di apparecchiature atte ad intercettare ed impedire comunicazioni informatiche commessi dal personale incaricato della gestione degli apparati e dei sistemi componenti l'infrastruttura di rete aziendale.

Art. 615-quinquies, 635 bis, 635 quater c.p.

Danneggiamento di informazioni, dati e programmi aziendali di un concorrente causato mediante la diffusione di virus o altri programmi malevoli commessa da soggetti che utilizzano abusivamente la rete o i sistemi di posta elettronica aziendali.

Danneggiamento di informazioni, dati, programmi informatici aziendali o di sistemi informatici di terzi, anche concorrenti, commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza.

Danneggiamento dei sistemi su cui i concorrenti conservano la documentazione relativa ai propri prodotti/progetti allo scopo di distruggere le informazioni e ottenere un vantaggio competitivo.

Danneggiamento delle infrastrutture tecnologiche dei concorrenti al fine di impedirne l'attività o danneggiarne l'immagine. Con riferimento a tali condotte, sono da considerarsi maggiormente esposti al rischio gli enti la cui

Formalizzazione di regole al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3).

Procedure per l'etichettatura e il trattamento delle informazioni in base allo schema di classificazione adottato dall'ente (A.7.2.2).

Controlli di individuazione, prevenzione e ripristino al fine di proteggere da *software* dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema (A.10.4.1).

Presenza di misure per un'adeguata protezione delle apparecchiature incustodite (A.11.3.2).

Previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business (A.11.6.2).

Procedure di controllo della installazione di *software* sui sistemi operativi (A.12.4.1). Procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).

<p>attività dipende strettamente dalle infrastrutture tecnologiche, come ad esempio avviene nell'e-commerce o e-banking.</p>	
<p>Art. 635-ter, 635 quinquies c.p. Danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), da parte di dipendenti di enti coinvolti a qualunque titolo in procedimenti o indagini giudiziarie. Danneggiamento di informazioni, dati e programmi informatici utilizzati da enti pubblici commesso dal personale incaricato della gestione dei sistemi di clienti della PA.</p>	<p>Formalizzazione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3). Procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione (A.7.2.2). Controlli di individuazione, prevenzione e ripristino al fine di proteggere da <i>software</i> dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema (A.10.4.1). Procedure di controllo della installazione di <i>software</i> sui sistemi operativi (A.12.4.1). Procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).</p>
<p>Art. 640-quinquies c.p. Rilascio di certificati digitali da parte di un ente certificatore senza che siano soddisfatti gli obblighi previsti dalla legge per il rilascio di certificati qualificati (es. identificabilità univoca del titolare, titolarità certificata), con lo scopo di mantenere un alto numero di certificati attivi. Aggiramento dei vincoli imposti dal sistema per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre così un guadagno all'ente.</p>	<p>Predisposizione di misure volte alla protezione dei documenti elettronici (es. firma digitale). Elaborazione di procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali.</p>

**Art. 24-ter d.lgs. 231/2001 - Delitti di criminalità organizzata Art. 10 l. 146/2006 - Ratifica ed esecuzione della
Convenzione ONU contro il crimine organizzato transnazionale**

Reati presupposto		
Codice penale	Art. 377-bis	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
	art. 378	Favoreggiamento personale
	art. 416	Associazione per delinquere
	art. 416 bis	Associazioni di tipo mafioso anche straniere
	art. 416 ter	Scambio elettorale politico-mafioso
	art. 630	Sequestro di persona a scopo di estorsione
Codice di procedura penale	art. 407, comma 2, lett. a), n. 5	Delitti in materia di armi
D.P.R. 309/1990 (T.U. stupefacenti)	art. 74	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope
D.P.R. 43/1973	Art. 291 quater	Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri

1. CONSIDERAZIONI

La legge 16 marzo 2006, n. 146, "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001", ha esteso la responsabilità degli enti ai reati di cd. criminalità organizzata transnazionale.

Lo scopo della Convenzione ONU così ratificata è di promuovere la cooperazione tra Stati al fine di prevenire e combattere il crimine organizzato transnazionale in maniera più efficace. Ogni Stato firmatario è chiamato ad adottare le misure necessarie, conformemente ai suoi principi giuridici, per determinare la responsabilità delle persone giuridiche che partecipano a reati gravi che coinvolgono un gruppo criminale organizzato.

La Convenzione ha lo scopo di armonizzare gli ordinamenti interni di tutti i Paesi affinché si possa affermare con certezza che un reato resti tale in qualsiasi paese. Gli impegni che i paesi di tutto il mondo devono assumere possono essere così sintetizzati:

- incriminare nelle legislazioni nazionali i reati di partecipazione ad associazione criminale, riciclaggio di denaro sporco, corruzione e intralcio alla giustizia;
 - stabilire la responsabilità degli enti e delle società per i fatti di reato indicati dal trattato;
 - adottare misure contro il riciclaggio di denaro sporco e i proventi delle attività criminali;
 - proteggere coloro che testimoniano contro il crimine organizzato;
 - rafforzare la cooperazione in ordine al trasferimento di giudizi, all'extradizione, al sequestro e alla confisca dei beni provenienti da reato o profitto del reato per rintracciare e giudicare gli indiziati;
 - incentivare la prevenzione della criminalità organizzata a livello nazionale e internazionale;
- fornire le necessarie risorse finanziarie a quei Paesi che richiedono assistenza per combattere congiuntamente la criminalità organizzata transnazionale.

L'art. 3 della legge n. 146 del 2006 definisce cosa debba intendersi per reato transnazionale al fine di individuare l'ambito di applicazione della normativa in esame.

In particolare, si considera reato transnazionale "il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato", nonché:

- sia commesso in più di uno Stato;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Per "gruppo criminale organizzato", ai sensi della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, si intende "un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi o reati stabiliti dalla convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale".

In linea generale, nell'ambito della più ampia definizione di reati di criminalità transnazionale e con riferimento ai reati presupposto della responsabilità dell'ente ex decreto 231, vengono in considerazione, ai sensi dell'art. 10 della legge n. 146 del 2006, le fattispecie delittuose concernenti i reati di associazione, i reati di traffico di migranti e di intralcio alla giustizia, a condizione che tali condotte delittuose siano state

commesse, nell'interesse o a vantaggio dell'ente, da soggetti che rivestono al suo interno un ruolo apicale o subordinato.

Nella sua formulazione originaria l'art. 10, commi 5 e 6, L. n. 146/2006, prevedeva l'estensione dell'ambito di applicazione del decreto 231 anche ai reati di riciclaggio e impiego di capitali di provenienza illecita se compiuti in ambito transnazionale. Con l'approvazione del decreto legislativo n. 231/2007, che ha disposto l'abrogazione di tali commi, la responsabilità amministrativa degli enti è stata estesa ai reati di ricettazione, riciclaggio e impiego di capitali di provenienza illecita indipendentemente dalla presenza o meno del requisito della transnazionalità (v. *infra* Scheda 12).

La legge di lotta al crimine organizzato transnazionale, con una clausola generale di chiusura (art. 10, comma 10), dispone l'applicabilità di tutte le disposizioni di cui al D.lgs. n. 231/2001 ai nuovi illeciti amministrativi imputabili all'ente.

Ai sensi dell'art. 24-ter, decreto 231, la responsabilità dell'ente può derivare, tra l'altro, dai reati associativi (artt. 416 e 416-bis c.p.) e dai delitti commessi avvalendosi del metodo mafioso ovvero al fine di agevolare l'attività dell'associazione criminosa o mafiosa.

Con riferimento ai reati associativi, l'art. 416 c.p. punisce coloro che promuovono, costituiscono o organizzano l'associazione allo scopo di commettere più delitti. Anche il solo fatto di partecipare all'associazione costituisce reato. La rilevanza penale delle condotte descritte dalla norma appare condizionata all'effettiva costituzione dell'associazione criminosa. Infatti, prima ancora di richiamare le singole condotte di promozione, costituzione, direzione, organizzazione ovvero di semplice partecipazione, la norma ne subordina la punibilità al momento in cui "tre o più persone" si siano effettivamente associate per commettere più delitti. Il delitto di associazione per delinquere si caratterizza quindi per l'autonomia dell'incriminazione rispetto agli eventuali reati successivamente commessi in attuazione del *pactum sceleris*. Tali eventuali delitti, infatti, concorrono con quello di associazione per delinquere e, se non perpetrati, lasciano sussistere il delitto previsto dall'art. 416 c.p.

L'associazione per delinquere, ad esempio, potrebbe venire in rilievo in collegamento con il reato di attività organizzata per il traffico illecito di rifiuti (art. 260 Codice dell'ambiente). Ciò impone all'impresa di prestare particolare attenzione alla selezione dei soggetti preposti alla gestione dei propri rifiuti.

Ai sensi dell'art. 416-bis c.p., l'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza intimidatrice del vincolo associativo e della condizione di assoggettamento e omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. Tale reato si caratterizza per l'utilizzazione, da parte degli associati, della forza intimidatrice e, dal lato passivo, per la condizione di assoggettamento e omertà, sia all'esterno che all'interno dell'associazione. In ottica 231, tutto questo dovrà comunque tramutarsi in condotte che rispondano a un interesse, o arrechino un oggettivo vantaggio, all'ente in questione.

Si evidenzia peraltro che l'ente potrebbe rispondere anche nel caso del c.d. "concorso esterno" nel reato associativo, vale a dire quando il soggetto apicale o sottoposto, fornisce un supporto all'associazione di tipo mafioso pur non prendendo parte al sodalizio criminale.

Al netto delle considerazioni sopra svolte, la configurazione dei reati associativi come reati-mezzo ha l'effetto di estendere la responsabilità dell'ente ex decreto 231 a una serie indefinita di fattispecie criminose commesse in attuazione del *pactum sceleris* e non necessariamente incluse nell'elenco dei reati presupposto. Si pensi, ad esempio, alla turbata libertà degli incanti (art. 353 c.p.), all'illecita concorrenza con violenza o minaccia (art. 513-bis, c.p.), all'inadempimento di contratti di pubbliche forniture (art. 355 c.p.) e alla frode nelle pubbliche forniture (art. 356 c.p.).

Pertanto, le diverse possibili manifestazioni dei reati presupposto considerati dall'art. 24-ter decreto 231, anche laddove di rilievo transnazionale, rendono necessaria una scrupolosa mappatura dei rischi, con particolare riferimento a quello di verifica di condotte dirette a favorire o recare vantaggio all'organizzazione criminale, nonché l'individuazione di adeguati controlli preventivi. A quest'ultimo proposito, ad esempio, la prevenzione dei delitti previsti dai richiamati articoli 355 e 356 c.p. presuppone il rafforzamento dei controlli nelle aree aziendali che si occupano dell'attività di fornitura pubblica di beni e servizi.

In linea generale, sul piano delle misure volte a prevenire i reati espressione del fenomeno della criminalità organizzata di tipo mafioso, è importante in primo luogo riferirsi ai presidi proposti nelle presenti Linee Guida in relazione ai singoli reati presupposto rilevanti e, inoltre, in considerazione della speciale pericolosità che caratterizza tali fattispecie, prevedere adeguati flussi informativi verso l'OdV e misure idonee a garantire la riservatezza dei soggetti che segnalano le violazioni, eventualmente anche mediante presidi specifici quali l'attivazione di una linea telefonica a ciò dedicata.

Nella stessa direzione, si evidenzia che l'adesione delle imprese associate a Confindustria al Protocollo di Legalità siglato il 10 maggio 2010 con il Ministero dell'Interno, e alle s.m.i., comporta l'adozione di misure che sono funzionali ad adeguare alla disciplina del decreto 231 gli assetti di gestione, organizzazione e controllo interno. Infatti, l'impresa aderente al Protocollo si impegna, ad esempio, a ottenere la documentazione antimafia liberatoria riguardante i propri fornitori e a richiedere loro il rispetto della tracciabilità dei flussi finanziari e la denuncia dei fenomeni estorsivi subiti. Come previsto dalla Commissione paritetica per la Legalità - istituita ai sensi del citato Protocollo - nelle Linee Guida attuative, tali procedure e misure preventive, se correttamente implementate e attuate, consentono di integrare il modello organizzativo per la parte relativa alla prevenzione dei reati di criminalità organizzata e di quelli affini (ad es. corruzione).

Con particolare riferimento al reato di associazione finalizzata al traffico illecito di stupefacenti (art. 74, DPR 9 ottobre 1990, n. 309), si rinvia ai controlli preventivi considerati rispetto ai reati associativi, con il *caveat* che si tratta di un reato raramente commesso nell'interesse o a vantaggio dell'ente.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Fattispecie incriminatrici - Aree a rischio reato	Controlli preventivi
<p>Art. 416, 416-bis c.p.; art. 291 -quater DPR 43/1973; art. 74 T.U. DPR 309/1990</p> <p>Selezione e assunzione del personale</p> <p>Selezione fornitori beni e servizi (ad es. servizi di ristorazione e pulizia)</p> <p>Conclusioni di contratti infragruppo di acquisto e/o di vendita.</p> <p>Gestione dei flussi finanziari.</p> <p>Investimenti infragruppo.</p>	<p>Adesione a Protocolli di legalità stipulati dalle associazioni di imprese e/o di categoria con il Ministero dell'Interno ovvero con le Prefetture territorialmente competenti e rispetto degli impegni conseguenti.</p> <p>Sigla di Protocolli di legalità tra l'impresa - o la sua sede operativa - e il Ministero dell'Interno o la locale Prefettura per lo svolgimento di verifiche antimafia su potenziali risorse da assumere e partner commerciali.</p> <p>Ai fini di una corretta selezione dei partner commerciali: i) introdurre meccanismi di qualificazione etica delle imprese, previsti dalla legge o da sistemi di autoregolamentazione, quali ad esempio: il possesso del <i>rating</i> di legalità; l'iscrizione nelle <i>white list</i> prefettizie o nell'elenco delle imprese aderenti al Protocollo di legalità tra Confindustria e il Ministero dell'Interno (v. sopra); ii) impegnare il fornitore a produrre una dichiarazione sostitutiva attestante il rispetto delle norme contributive, fiscali, previdenziali e assicurative a favore dei propri dipendenti e collaboratori, degli obblighi di tracciabilità finanziaria, nonché l'assenza di provvedimenti a carico dell'ente o dei suoi apicali per reati della specie di quelli previsti dal decreto 231, con particolare riferimento a quelli di cui all'art. 24-ter. Nei contratti con i fornitori: i) clausola risolutiva espressa per il caso in cui l'impresa fornitrice, destinataria di una certificazione antimafia regolare, risulti destinataria di una sopraggiunta comunicazione ovvero informazione antimafia interdittiva, nonché per l'ipotesi di mancato rispetto delle norme richiamate al punto i) precedente e dell'obbligo di denunciare i reati subito direttamente o dai propri familiari e/o collaboratori; ii) limitazione al tempo strettamente necessario del termine entro cui il fornitore destinatario di una sopraggiunta informazione antimafia interdittiva viene in concreto estromesso dal contratto. Rotazione periodica del personale addetto alle aree e funzioni a maggiore rischio di reato.</p> <p>Adozione da parte delle società estere del Gruppo di procedure o sistemi di controllo interno compatibili con quelli previsti dal modello organizzativo ex decreto 231.</p> <p>Applicazione dei controlli preventivi specifici (protocolli) previsti anche in riferimento ai reati nei rapporti con la Pubblica Amministrazione, ai reati societari e ai reati di <i>market abuse</i>.</p> <p>Verifica preventiva (ad es. mediante obbligo di dichiarazione sostitutiva) dell'inesistenza di vincoli di parentela o affinità tra gli esponenti della società nominati negli organi sociali di controllate estere e gli esponenti della pubblica amministrazione locale e/o fornitori, clienti o terzi contraenti della società medesima.</p>

<p>Designazione membri degli organi sociali in società estere da parte della capogruppo.</p> <p>Contratti di acquisto e/o di vendita con controparti estere.</p> <p>Transazioni finanziarie con controparti estere.</p> <p>Investimenti con controparti estere.</p>	<p>Verifica che i partner commerciali/finanziari esteri posseggano i requisiti di onorabilità e professionalità e non siano presenti nelle Liste dei soggetti designati, destinatari delle misure di congelamento di fondi e risorse economiche (in base a regolamenti comunitari o provvedimenti nazionali), consultabili sul sito internet di Banca d'Italia, sezione Unità di informazione finanziaria - UIF.</p> <p>Controlli formali e sostanziali dei flussi finanziari aziendali.</p> <p>Determinazione dei criteri di selezione, stipulazione ed esecuzione di <i>accordi/joint-ventures</i> con altre imprese estere per la realizzazione di investimenti e previsione di meccanismi per assicurarne trasparenza e tracciabilità.</p>
<p>Art. 377-bis, 378 c.p.</p> <p>Rapporti con soggetti coinvolti in procedimenti giudiziari.</p>	<p>di Comunicazione all'Ufficio legale della notizia o della notifica dell'indagine.</p>

Art. 25 d.lgs. 231/2001 - Concussione, induzione indebita a dare o promettere utilità e corruzione

Reati presupposto		
Codice penale	art. 317	Concussione
	art. 318	Corruzione per l'esercizio della funzione
	art. 319	Corruzione per un atto contrario ai doveri di ufficio
	art. 319 ter	Corruzione in atti giudiziari
	art. 319 quater	Induzione indebita a dare o promettere utilità
	art. 321	Pene per il corruttore
	art. 322	Istigazione alla corruzione

1. CONSIDERAZIONI GENERALI

Si tratta di tipologie di reato che rientrano nell'ambito dei reati contro la Pubblica Amministrazione e, in quanto tali, presuppongono l'instaurazione di rapporti con soggetti pubblici e/o l'esercizio di una pubblica funzione o di un pubblico servizio.

Si è, in particolare, in presenza di reati propri, il cui soggetto attivo è di regola un pubblico funzionario. L'inserimento come delitto presupposto nel decreto 231 (art. 25) si giustifica poiché la legge punisce - in presenza di determinate circostanze - anche il privato che concorre con il soggetto pubblico nella realizzazione del reato, come nel caso di induzione indebita a dare o promettere utilità o della corruzione attiva, su cui ci si soffermerà in seguito.

Inoltre, nel nostro ordinamento non è raro che la qualità di soggetto pubblico (pubblico ufficiale e incaricato di pubblico servizio) sia estesa anche nei confronti di soggetti privati e, quindi, che tale qualifica sia attribuita ad esponenti di realtà societarie a carattere privato, investite dello svolgimento di pubblici servizi o di pubbliche funzioni, nei limiti e in relazione alle attività aziendali riconducibili all'assolvimento di tali compiti, come anche di seguito specificato.

A tale proposito si deve ricordare che, secondo l'attuale disciplina, ciò che rileva è, infatti, l'attività svolta in concreto e non la natura giuridica, pubblica o privata, del soggetto. Ne consegue che il nostro ordinamento accoglie una nozione di pubblico ufficiale e di incaricato di pubblico servizio di tipo "oggettivo", che comporta la necessità di una valutazione "caso per caso" - peraltro non sempre agevole - delle singole funzioni ed attività svolte, sia per determinare la qualificazione del soggetto interessato (pubblico ufficiale, incaricato di pubblico servizio o semplice privato)

sia, di conseguenza, per stabilire la natura delle azioni realizzate dal medesimo. Da ciò discende che possono coesistere in capo ad un medesimo soggetto, almeno a fini penalistici, qualifiche soggettive diverse.

Pertanto, al fine di valutare i possibili ambiti aziendali esposti a maggior rischio è necessario premettere che:

- i. la qualifica di pubblico ufficiale (art. 357 c.p.) va riconosciuta a tutti i soggetti, pubblici dipendenti o privati, che possono o debbono, nell'ambito di una potestà regolata dal diritto pubblico, formare e manifestare la volontà della Pubblica Amministrazione ovvero esercitare poteri autoritativi o certificativi (es. recapito degli atti giudiziari o attività di messo notificatore per conto di Equitalia o di amministrazioni comunali; concessione finanziamenti agevolati per conto dei Ministeri; riscossione coattiva tributi; etc.);
- ii. sono incaricati di un pubblico servizio (art. 358 c.p.) coloro i quali, a qualunque titolo, prestano un pubblico servizio e che, pur agendo nell'ambito di un'attività disciplinata nelle forme della pubblica funzione, mancano dei poteri tipici di questa, con esclusione dello svolgimento di semplici mansioni d'ordine o di prestazione di un'attività meramente materiale (es. erogazione servizi di vario tipo sulla base di convenzioni con Ministeri o altri soggetti annoverabili tra le PA che non comportino poteri certificativi) .

In conclusione è possibile dedurre che, limitando per il momento l'analisi ai soli reati di natura corruttiva, in taluni casi possono configurarsi sia corruzioni c.d. attive (es. l'amministratore o il dipendente della singola società corrompe un pubblico ufficiale o un incaricato di pubblico servizio per far ottenere all'ente qualcosa), sia corruzioni c.d. passive (es. l'esponente dell'ente - nello svolgimento di un'attività di natura "pubblicistica" - riceve denaro per compiere un atto contrario ai doveri del proprio ufficio). Tale ultima forma d'illecito, nell'ottica del decreto 231, si verificherà con minore frequenza della prima, giacché nella maggior parte dei casi si tratterà di corruzioni realizzate nell'esclusivo interesse della persona fisica senza, cioè, che sia configurabile un *interesse o vantaggio* dell'ente. Tuttavia, anche in questi casi, non è possibile escludere che si verifichino ipotesi di corruzione passiva che generano responsabilità dell'ente (ad es. laddove quest'ultimo abbia tratto un vantaggio - eventualmente anche indiretto - dalla commissione del reato da parte del proprio esponente) e ciò, verosimilmente, si potrà verificare proprio con riferimento a quei soggetti, di diritto privato o di diritto pubblico (ad es. i c.d. enti pubblici economici) la cui attività sia, in tutto o in parte, da considerare come pubblica funzione o pubblico servizio.

Per quanto riguarda il reato di corruzione in atti giudiziari (art. 319 *ter* c.p.), si precisa che tale fattispecie non ricorre soltanto in relazione all'esercizio delle funzioni giudiziarie cui è subordinata e allo status di colui che le esercita, ma ha una portata più ampia. Infatti, come precisato dalla Corte di Cassazione, costituisce "atto giudiziario" qualsiasi atto funzionale a un procedimento giudiziario, indipendentemente dalla qualifica soggettiva di chi lo realizza (cfr. Cass., Sezioni Unite, sentenza n. 15.208 del 25/2/2010, con riferimento alla testimonianza resa in un processo penale).

Nell'ambito dei reati in esame, è recentemente intervenuta la legge 6 novembre 2012, n. 190 contenente nuove "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" (cd. Legge anticorruzione).

Tale provvedimento (di ratifica della convenzione di Strasburgo del 1999), oltre a determinare importanti effetti nel più ampio contesto normativo, in ottica di un complessivo rafforzamento degli strumenti volti a contrastare i fenomeni corruttivi, anche mediante un inasprimento del trattamento

sanzionatorio per gli autori dei diversi reati interessati, e a favorire la maggiore trasparenza nell'azione amministrativa, ha introdotto importanti novità, con significativi riflessi anche nella specifica materia del D.lgs. n. 231/01. In particolare:

- la concussione (art. 317 c.p.) è ora riferibile soltanto alla figura del pubblico ufficiale e circoscritta alle sole ipotesi in cui vi sia la costrizione del privato;
- la distinta ipotesi di concussione per induzione, precedentemente prevista nell'ambito dell'articolo 317 c.p., ha acquisito rilievo di fattispecie autonoma mediante l'introduzione del nuovo reato di induzione indebita a dare o promettere utilità (art. 319-quater c.p.). L'aspetto più significativo della modifica normativa nella prospettiva della responsabilità dell'ente è che soggetto attivo del delitto in esame è anche il soggetto privato che partecipa al reato corrispondendo o impegnandosi a dare l'utilità, nonostante le pene riservate al privato siano più miti di quelle previste per il pubblico ufficiale o l'incaricato di pubblico servizio;
- nel contempo, il legislatore ha provveduto a rimodulare il reato di corruzione con l'inserimento, tra l'altro, della corruzione per l'esercizio della funzione (art. 318 c.p.) in luogo del precedente reato di corruzione per un atto d'ufficio. Il nuovo reato risulta configurabile laddove vi sia un flusso illecito di denaro (o altra utilità) tra esponenti aziendali e un soggetto pubblico, nell'esercizio delle proprie funzioni o dei suoi poteri, senza la necessità che sia dimostrato (come invece richiesto dalla formulazione precedente del reato) un nesso causale tra la prestazione (o l'utilità erogata) e un singolo e specifico provvedimento o atto della PA.

Ai fini della costruzione del modello organizzativo, è importante distinguere le fattispecie in esame e considerarne le differenti caratteristiche strutturali. Al riguardo, la Corte di Cassazione (Sezioni Unite, sentenza n. 12228 del 14 marzo 2014) ha indicato i principi di diritto da osservare per individuare la linea di confine tra i diversi illeciti, evidenziando che:

- i. la differenza tra il reato di concussione (art. 317 c.p.) e quello di induzione indebita a dare o promettere utilità (319-quater c.p.) riguarda i soggetti attivi e le modalità di perseguimento del risultato o della promessa di utilità. Infatti, la concussione consiste nell'abuso costrittivo attuato dal pubblico ufficiale mediante violenza o minaccia di un danno *contra ius* che determina la soggezione psicologica del destinatario -ma non l'annullamento della sua libertà di autodeterminazione - il quale, senza riceverne alcun vantaggio, si trova di fronte all'alternativa di subire il male prospettato o di evitarlo con la dazione o promessa dell'utilità. L'induzione indebita si realizza, invece, nel caso di abuso induttivo del pubblico ufficiale o incaricato di pubblico servizio che, con una condotta di persuasione, inganno o pressione morale condiziona in modo più tenue la volontà del destinatario; quest'ultimo, pur disponendo di un margine decisionale più ampio, finisce per accettare la richiesta della prestazione indebita, nella prospettiva di conseguire un tornaconto personale;
- ii. i reati di concussione e induzione indebita si distinguono dalle fattispecie corruttive in quanto i primi due delitti presuppongono una condotta di prevaricazione abusiva del funzionario pubblico idonea a determinare la soggezione psicologica del privato, costretto o indotto alla dazione o promessa indebita, mentre l'accordo corruttivo viene concluso liberamente e consapevolmente dalle parti. Queste si trovano su un piano di parità sinallagmatica, nel senso che l'accordo è in grado di produrre vantaggi reciproci per entrambi i soggetti che lo pongano in essere. In tale ambito è inoltre opportuno segnalare, in ragione del suo carattere innovativo, l'introduzione della fattispecie inerente il reato di *traffico di*

influenze illecite (art. 346-bis c.p.). Pur non costituendo detto reato presupposto per la responsabilità degli enti ai sensi del decreto 231, si ritiene che esso assuma - nel generale contesto delineato dal vigente quadro normativo, che recepisce gli orientamenti internazionali sul contrasto anche di comportamenti prodromici rispetto ad accordi corruttivi - particolare rilevanza, in quanto le relative condotte illecite potrebbero avere un carattere di connessione e/o di contiguità rispetto a quelle corruttive, rilevanti nell'ottica del decreto 231.

Le profonde modifiche intervenute per effetto dell'introduzione della nuova normativa comportano la necessità di una revisione dei modelli organizzativi precedentemente elaborati dalle imprese ai fini del decreto 231, così da aggiornare l'individuazione degli ambiti (attività, funzioni, processi) in relazione al nuovo quadro normativo che si è delineato.

Al riguardo si può affermare - a livello orientativo - che la nuova normativa, e in particolare l'introduzione *ex novo* del delitto di induzione indebita a dare o promettere utilità, possa comportare, ferma restando la specificità di ogni singolo contesto aziendale, l'ampliamento in termini significativi delle aree di attività potenzialmente sensibili.

Infatti, considerato che il predetto delitto prevede l'estensione della punibilità anche al soggetto (privato) "indotto" dall'esponente pubblico alla corresponsione dell'utilità (con un elemento di forte discontinuità rispetto al precedente reato di concussione che vedeva nel soggetto privato esclusivamente una "vittima" del reato), le aree aziendali di potenziale esposizione al rischio tenderanno a comprendere tutti gli ambiti di operatività contraddistinti da rapporti con soggetti pubblici (oltre che le attività eventualmente svolte da parte di un esponente dell'azienda in qualità di pubblico ufficiale o di incaricato di pubblico servizio in veste, in tal caso, di colui che "induce" alla prestazione indebita), con un ampliamento delle aree interessate dal precedente reato di concussione per induzione.

Un ampliamento dell'ambito della responsabilità, sia per il privato che per il pubblico ufficiale, è stato poi realizzato anche con la novella dell'articolo 318 del codice penale. Innanzitutto, come accennato, la fattispecie rinuncia oggi al requisito della strumentalità dell'accordo rispetto a un predeterminato atto dell'ufficio (risulta, ad esempio, punibile anche solo l'asservimento della funzione alle esigenze del corruttore). In secondo luogo, nella corruzione per l'esercizio della funzione confluiscono anche le originarie ipotesi di corruzione impropria attiva susseguente non punite, sul versante privato, nella precedente disciplina. Infine, nel novellato articolo 318 è venuto meno il riferimento al concetto di retribuzione e si porrà dunque il problema interpretativo della possibile estensione della punibilità anche alle dazioni di regalie e donativi d'uso.

Per quanto attiene, invece, la nuova formulazione del reato di concussione (ora previsto limitatamente alla realizzazione di una condotta caratterizzata dalla sola costrizione), è ipotizzabile che lo stesso assuma connotazioni residuali rispetto al passato, in ragione sia della particolare configurabilità di un interesse o un vantaggio da parte dell'ente in relazione a tale tipologia di reato (ravvisabile solo in determinati contesti operativi), sia dell'elemento soggettivo ricondotto alla sola figura del pubblico ufficiale, oltre che in considerazione delle specifiche modalità richieste per la realizzazione stessa del reato (il ricorso a comportamenti costrittivi).

Relativamente all'ambito dei reati corruttivi, si è già sottolineata la significatività dell'introduzione della nuova fattispecie di reato di corruzione per l'esercizio della funzione, in luogo della precedente ipotesi di corruzione per un atto d'ufficio.

Al riguardo, si può ritenere che, nel nuovo contesto, acquisiscano significativa rilevanza le aree di attività aziendale che comportano rapporti con la P.A. (Ministeri, Enti Pubblici, Autorità di Vigilanza, ecc.), in particolare - ma non in via esclusiva - laddove tali rapporti assumano un carattere di continuità. In tale ambito, tra l'altro, dovrà essere rivolta specifica attenzione alle politiche aziendali finalizzate alla corresponsione di prestazioni a titolo gratuito (omaggi, donazioni, atti di cortesia, ecc.), laddove siano elargite nei confronti di soggetti pubblici.

Sono altresì da considerare a rischio ulteriori attività (quali, a titolo esemplificativo, i processi di selezione e assunzione del personale, l'attività di selezione, negoziazione, stipula ed esecuzione di contratti di acquisto riferita a soggetti privati, la gestione delle risorse finanziarie, ecc.) che, pur non comportando contatti o rapporti diretti con la P.A., potrebbero assumere carattere strumentale e/o di supporto ai fini della commissione dei reati di corruzione e di induzione indebita a dare o promettere utilità. Si tratta, infatti, di processi che, anche se svolti nell'ambito di rapporti tra privati, possono risultare strumentali ai fini della costituzione di una "provvista" da impiegarsi per successive attività corruttive (ovvero consentono il riconoscimento di un'utilità diversa dal denaro a titolo di favore verso un soggetto della P.A.).

In tale contesto, rivestono particolare significatività in ottica 231 le prestazioni di servizi a carattere immateriale (tra cui le consulenze, ma anche le iniziative di sponsorizzazione, le manutenzioni o i servizi accessori eventualmente correlati alle forniture di beni), nonché le offerte commerciali cd. non standard che comportano, pertanto, profili di *customizzazione*; in tali casi, infatti, i margini di discrezionalità (sia del corrotto che del corruttore) per occultare un'ingiustificata maggiorazione dei prezzi, tipicamente effettuata dall'azienda venditrice per rientrare del costo dell'azione corruttiva, si presentano normalmente più ampi.

Infine, con riferimento a operazioni economiche transfrontaliere, si evidenzia la necessità di prevedere specifici controlli per prevenire i reati in esame laddove commessi, nell'interesse o vantaggio dell'impresa, nei confronti di soggetti stranieri che siano pubblici ufficiali o incaricati di pubblico servizio (v. art. 322-bis c.p.). In particolare, il corruttore (art. 321 c.p.), chi ha posto in essere una condotta di istigazione alla corruzione (art. 322, co. 1 e 2 c.p.) e chi ha dato o promesso un'utilità a seguito a un'induzione indebita (art. 319-*quater* c.p.) è sempre punibile per i fatti commessi nei confronti di: i) pubblici ufficiali o incaricati di pubblico servizio di ambito europeo; ii) persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali o degli incaricati di pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, se il fatto è commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali o per mantenere una attività economica o finanziaria.

Premesso quanto sopra, si rinvia alla tabella predisposta nelle pagine seguenti, in via meramente esemplificativa e non esaustiva, le principali macro aree da considerarsi direttamente a rischio reato, con l'evidenziazione di alcuni possibili presidi e controlli preventivi da implementare nel contesto aziendale, nell'ambito di un organico sistema procedurale, ai fini della loro copertura. Detti presidi, da calibrare in funzione delle caratterizzazioni e dimensioni di ciascuna impresa, integrano o si aggiungono alle misure preventive comuni a tutte le aree di rischio reato.

In materia di controlli specifici si rileva che anche le attività di monitoraggio, tipicamente svolte a valle delle operazioni, possono sortire un effetto di "prevenzione" agendo come deterrente rispetto ad azioni illecite.

Il "*Bribery Act*" ed il Modello di Organizzazione previsto dal decreto 231

Con l'entrata in vigore del "*Bribery Act*" il 1° luglio 2011, è stata introdotta nel Regno Unito una nuova disciplina in materia di corruzione. Essa estende i profili di responsabilità penale alle persone giuridiche sia per i reati di corruzione commessi da soggetti che operano in nome e per conto delle medesime sia per il reato di mancata prevenzione della corruzione.

Sia il *Bribery Act* sia il decreto 231 nascono a valle di accordi internazionali e di Convenzioni (OCSE) e questo, probabilmente, ne ha favorito le evidenti similitudini, sebbene sussistano alcune differenze.

Entrambi i corpi normativi contengono e disciplinano le responsabilità delle persone giuridiche in ordine a reati di corruzione ma mentre il *Bribery Act* si riferisce in modo pressoché esclusivo ai reati di corruzione, il nostro sistema 231 si estende a diverse e numerose categorie di reato, in costante ampliamento.

Le sanzioni di cui al *Bribery Act* nei confronti delle persone giuridiche sono sanzioni penali anche formalmente (*Criminal Fines*); non può dirsi lo stesso delle corrispondenti sanzioni di cui al decreto 231. Inoltre, mentre quest'ultime possono essere di natura economica e/o interdittive e sono applicabili nell'ambito di un minimo ed un massimo predeterminati dalla legge, il *Bribery Act* non fissa un limite predeterminato alle sanzioni, che sono esclusivamente di natura economica, lasciando che la loro quantificazione venga determinata in termini di proporzionalità alla gravità della condotta.

Da rilevarsi, inoltre, che il *Bribery Act* prevede e disciplina anche la cd. corruzione privata, solo di recente introdotta nel nostro ordinamento per effetto della già richiamata legge n. 190 del 2012 che ne ha contestualmente previsto l'inserimento nel decreto (art. 25-ter, lett. s-bis)³.

Un elemento di similitudine tra i due sistemi è il presupposto della responsabilità dell'ente che si fonda in entrambi sull'interesse o il vantaggio derivante all'ente stesso dalla commissione dell'illecito.

Il *Bribery Act* si applica sia alle compagnie inglesi operanti in Gran Bretagna così come fuori della stessa (es. in Italia) ma anche alle compagnie straniere (es. italiane) operanti in Gran Bretagna.

³ In relazione al reato di *corruzione tra privati*, previsto dall'art. 2635 del codice civile, si veda l'apposito approfondimento nell'ambito dell'area dedicata ai reati societari.

Sistema di prevenzione - Linee Guida

Sia il *Bribery Act* sia il nostro decreto 231 prevedono quale esimente della responsabilità "penale" delle persone giuridiche l'adozione di un efficace modello di organizzazione teso a prevenire la commissione dei reati.

Al riguardo è interessante notare che mentre il decreto 231 attribuisce alle principali associazioni di categoria il compito di formulare Linee Guida che, valutate positivamente dal Ministero della Giustizia, possano essere validamente ed efficacemente adottate dalla singole imprese per la realizzazione dei propri modelli organizzativi, in Gran Bretagna tali Linee Guida sono state emesse direttamente da parte del Governo (marzo 2011).

I due sistemi di organizzazione gestione e controllo sono confrontabili sotto diversi punti di vista.

Entrambi si fondano su un preliminare *risk assessment* dell'azienda, del suo business, dei settori e delle attività che la caratterizzano al fine di valutare se e quali siano i rischi di commissione di reati in seno alla organizzazione aziendale.

Il *Bribery Act* stabilisce in linea generale quello che risulta puntualmente disciplinato dalle Linee Guida italiane in ordine alla necessità che il Modello sia adottato dal Consiglio di Amministrazione della società e comunque dai vertici della stessa unitamente ad un appropriato e coerente Codice Etico.

Necessario corollario del principio sopra enunciato è costituito, sia nel *Bribery Act* sia nel nostro sistema, dall'adozione di *policies* e procedure che non solo disciplinino i rapporti all'interno dell'azienda e dei dipendenti dell'azienda stessa, ma anche i rapporti con i terzi (*partners*, agenti, fornitori, rivenditori, ecc.).

In particolare, mentre il *Bribery Act* prevede l'adozione di specifiche procedure solo riguardo i reati di corruzione, il nostro sistema attuale può considerarsi un generale sistema di prevenzione dei reati e, in quanto tale, necessariamente ricomprende procedure specifiche anche in materia di contrasto alla corruzione.

Infine, sono comuni ai due sistemi, al fine di garantire una concreta efficacia prevenzionistica dei modelli di organizzazione gestione e controllo:

l'importanza della predisposizione di un sistema sanzionatorio o l'integrazione di quello già esistente in relazione ad eventuali violazioni del modello di organizzazione.

la generale diffusione interna ed esterna del modello adottato e del codice etico;

la necessaria informazione e formazione del personale;

la creazione di un organismo che verifichi la corretta implementazione del modello, ne curi il continuo aggiornamento e comunichi periodicamente le conclusioni sull'attività svolta al vertice dell'azienda.

Opportunità

Il *Bribery Act* è molto chiaro nel disporre che chiunque faccia affari nel Regno Unito, a prescindere dalla sede dell'impresa, dovrà adeguarsi ai principi normativi in esso espressi. Pertanto, le società italiane che hanno sedi secondarie, società controllate o che semplicemente svolgono un'attività commerciale di vendita o di prestazione di servizi nel Regno Unito, se vorranno evitare le sanzioni pecuniarie che la legge inglese prevede quale conseguenza della commissione di reati di corruzione o alla loro mancata prevenzione, dovranno dotarsi di adeguate procedure che, in parte, potranno essere mutate dal modello di organizzazione e gestione già adottato in conformità a quanto previsto dal nostro decreto 231. È evidente l'opportunità quindi che si presenta alle aziende italiane di verificare il proprio Modello di Organizzazione ex decreto 231 e ove occorra integrarlo alla luce dei principi propri del *Bribery Act* così da consentirne un utile impiego, esteso alle previsioni normative di quest'ultimo.

In tale direzione, e del tutto parallelamente alla precedente verifica e ad una sua eventuale integrazione, appaiono indispensabili specifici programmi di formazione con particolare riguardo alle funzioni e ruoli aziendali maggiormente esposti al rischio di commissione di reati corruttivi, valutato in una prospettiva internazionale.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Aree a rischio reato	Controlli preventivi
<p>Partecipazione a procedure di gara o di negoziazione diretta per la vendita di beni e servizi o finalizzate alla realizzazione di opere a favore della PA, nonché la successiva attività di erogazione del servizio e/o della prevista prestazione contrattuale.</p> <p>Attività funzionalmente connesse con l'esercizio, da parte dell'ente, di compiti di natura pubblicistica in quanto correlate all'esercizio di una funzione pubblica o di un pubblico servizio.</p> <p>Realizzazione di accordi di <i>partnership</i> con terzi soggetti per collaborazioni commerciali e, in generale, il ricorso ad attività di intermediazione finalizzate alla vendita di prodotti e/o servizi nei confronti di soggetti pubblici nazionali.</p> <p>Rapporti con: • Autorità Indipendenti e di Vigilanza e altri organismi di diritto pubblico;</p> <p>• pubblici ufficiali e incaricati di pubblico servizio relativamente agli adempimenti fiscali, tributari e previdenziali;</p>	<p>Monitoraggio delle offerte economiche relative a gare e a trattative private con la PA, corredato da analisi del <i>trend</i> dei prezzi praticati, nonché monitoraggio delle fasi evolutive dei procedimenti di gara o di negoziazione diretta.</p> <p><i>Reporting</i> interno, a fronte delle attività di monitoraggio, per favorire sistemi di <i>cross control</i> e gestione delle anomalie tra le diverse funzioni aziendali.</p> <p>Procedure di tracciabilità dei flussi finanziari aziendali con l'individuazione dei soggetti autorizzati all'accesso alle risorse.</p> <p>Verifiche, a cura di idonee funzioni aziendali distinte da quella "commerciale", sull'effettiva erogazione delle forniture e/o sulla reale prestazione dei servizi, inclusi i controlli sui livelli qualitativi attesi, anche ai fini della risoluzione di possibili contestazioni del cliente a fronte di ipotesi di disservizi.</p> <p>Presidi specifici a fronte del ricorso a <i>partnership</i> commerciali, intermediazioni e forme aggregative tra imprese quali, ad es. ricorso ad attestazioni in ottica 231, attivazione sistemi di monitoraggio gestionale estesi alle aree di interesse, etc.</p>

<ul style="list-style-type: none"> • Autorità Giudiziaria, pubblici ufficiali e incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale. <p>La partecipazione a procedure per l'ottenimento di licenze, provvedimenti amministrativi ed autorizzazioni da parte della PA.</p> <p>Le attività di acquisto dalla PA, ovvero le attività di acquisto svolte con la qualifica di pubblica funzione o incaricato di pubblico servizio.</p> <p>La partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto utilizzo.</p> <p>Selezione e assunzione del personale.</p> <p>Gestione delle finanziarie e di strumenti finanziari derivati.</p> <p>Gestione delle posizioni creditorie e delle iniziative di recupero delle stesse (in relazione a ipotesi di stralci di credito, parziali o totali), nonché le transazioni commerciali remissive a fronte di disservizi e contestazioni.</p>	<p>Controlli dei collaboratori esterni (ad esempio agenti) e della congruità delle provvigioni pagate rispetto a quelle praticate nell'area geografica di riferimento.</p> <p>Monitoraggio dei procedimenti di richiesta di erogazioni, contributi o finanziamenti pubblici e attivazione di approfondimenti su potenziali indicatori di rischio (es. concentrazione richieste andate a buon fine su determinati soggetti PA).</p>
<p>Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, riferita a soggetti privati, con particolare riferimento al ricevimento di beni e attività finalizzate all'attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento specialmente in relazione ad acquisti di natura immateriale, tra cui:</p> <ul style="list-style-type: none"> • consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto; • pubblicità; • sponsorizzazioni; • spese di rappresentanza; • locazioni passive; • attività di sviluppo di software e servizi ICT. 	<p>Predisposizione di specifiche procedure organizzative relative ad acquisti, consulenze, sponsorizzazioni, reclutamento del personale, spese di rappresentanza, Linee Guida per la gestione della finanza aziendale, ecc.), assicurando per esempio:</p> <ul style="list-style-type: none"> • verifiche preventive sulle controparti o sui beneficiari; • definizione di criteri qualitativi/quantitativi con adeguati livelli di autorizzazione per le spese di rappresentanza; • distinzione dei ruoli; stratificazione dei poteri di firma; tracciabilità dei flussi finanziari.

<p>Partecipazione a procedure di gara o di negoziazione diretta, indette da organismi pubblici dell'Unione Europea o stranieri o a similari procedure svolte in un contesto competitivo a carattere internazionale.</p>	<p>Procedimentalizzazione dei rapporti e delle operazioni che si svolgono nelle aree geografiche a maggiore rischio reato, eventualmente adottando particolari cautele già nella fase precontrattuale e di negoziazione, nonché nella individuazione dei soggetti incaricati delle relative operazioni e nello scambio di comunicazioni formali che ne attestino la trasparenza e correttezza.</p> <p>Consultazione di studi e rilievi analitici, ormai consolidati e di particolare attendibilità, che periodicamente enti specializzati svolgono per valutare il livello di corruzione nelle pubbliche amministrazioni in tutti i paesi del mondo.</p>
<p>Partecipazione a procedure di evidenza pubblica in associazione con altri partner (RTI, ATI, <i>joint venture</i>, consorzi, etc.).</p>	<p>Per evitare la propagazione di responsabilità agli enti che abbiano realizzato forme di associazione con altri partner commerciali, a fronte di un illecito corruttivo commesso dall'esponente di uno di questi ultimi, può essere utile:</p> <ul style="list-style-type: none"> la conduzione di adeguate verifiche preventive sui potenziali partner; la previsione di un omogeneo approccio e di una condivisa sensibilità da parte dei componenti dell'ATI/RTI o dei consorziati o intermediari sui temi afferenti la corretta applicazione del decreto 231, anche in relazione all'adozione di un proprio modello organizzativo da parte di ciascun componente del raggruppamento nonché all'impegno, esteso a tutti i soggetti coinvolti, di adottare un proprio Codice Etico; acquisizione dai partner di informazioni sul sistema dei presidi dagli stessi implementato, nonché flussi di informazione tesi ad alimentare un monitoraggio gestionale, ovvero attestazioni periodiche sigli ambiti di rilevanza 231 di interesse (es. attestazioni rilasciate con cadenza periodica in cui ciascun partner dichiara di non essere a conoscenza di informazioni o situazioni che possano, direttamente o indirettamente, configurare le ipotesi di reato previste dal decreto 231); eventuale definizione di specifiche clausole contrattuali di audit (da svolgere sia con idonee strutture presenti all'interno dell'aggregazione tra imprese che con l'eventuale ricorso a soggetti esterni), da attivarsi a fronte di eventuali indicatori di rischio rilevati; adozione, accanto al Codice Etico, di uno specifico Codice di Comportamento rivolto ai fornitori e partner che contenga le regole etico-sociali destinate a disciplinare i rapporti dei suddetti soggetti con l'impresa, cui auspicabilmente aderiscano le controparti che affiancano la società nelle diverse opportunità di <i>business</i> (es. <i>joint venture</i>, ATI, RTI, consorzi, etc.).

Art. 25 *bis* d.lgs. 231/2001 - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Art. 25 bis.1 d.lgs. 231/2001 - Delitti contro l'industria e il commercio

Reati presupposto

Codice penale	art. 453	Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate
	art. 454	Alterazione di monete
	art. 455	Spendita e introduzione nello Stato, senza concerto, di monete falsificate
	art. 457	Spendita di monete falsificate ricevute in buona fede
	art. 459	Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati
	art. 460	Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo
	art. 461	Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata
	art. 464	Uso di valori di bollo contraffatti o alterati
	art. 473	Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni
	art. 474	Introduzione nello Stato e commercio di prodotti con segni falsi
	art. 513	Turbata libertà dell'industria o del commercio
	art. 513 <i>bis</i>	Illecita concorrenza con minaccia o violenza
	art. 514	Frodi contro le industrie nazionali
	art. 515	Frode nell'esercizio del commercio
	art. 516	Vendita di sostanze alimentari non genuine come genuine
	art. 517	Vendita di prodotti industriali con segni mendaci
art. 517 <i>ter</i>	Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale	
art. 517 <i>quater</i>	Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari	

1. CONSIDERAZIONI GENERALI

Al fine di perseguire la prevenzione dei reati di falsità in strumenti o segni di riconoscimento possono osservarsi i seguenti principi:

- qualora sia rilevato il rischio di svolgere attività che potrebbero entrare in contrasto e, quindi, violare, diritti di proprietà industriale spettanti a terzi (tra cui l'utilizzazione di tecnologie coperte da brevetto già depositato), occorre svolgere una previa verifica su precedenti brevetti e marchi registrati a nome di terzi;
- inserire nei contratti di acquisizione di prodotti tutelati da diritti di proprietà industriale specifiche clausole con cui la controparte attesti:
 - di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
 - che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà industriale in capo a terzi;
 - che si impegna a manlevare e tenere indenne la società da qualsivoglia danno o pregiudizio per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

Occorre invece evitare di:

- utilizzare segreti aziendali altrui;
- adottare condotte finalizzate ad intralciare il normale funzionamento delle attività economiche e commerciali di società concorrenti di la società;
- porre in essere atti fraudolenti idonei a produrre uno sviamento della clientela altrui e un danno per le imprese concorrenti alla società;
- riprodurre abusivamente, imitare, manomettere marchi, segni distintivi, brevetti, disegni industriali o modelli in titolarità di terzi;
- fare uso, in ambito industriale e/o commerciale, di marchi, segni distintivi, brevetti, disegni industriali o modelli contraffatti da soggetti terzi;
- introdurre nel territorio dello Stato per farne commercio, detenere per vendere o mettere in qualunque modo in circolazione prodotti industriali con marchi o segni distintivi contraffatti o alterati da soggetti terzi.

In generale, la prevenzione dei reati di falsità in strumenti o segni di riconoscimento è svolta attraverso adeguate misure organizzative e normative e in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- previsione nel codice etico e relativa appendice applicativa di specifiche indicazioni volte a impedire la commissione dei reati previsti dagli articoli *25-bis* e *25-bis.1* ;

- previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del modello) che violino i sistemi di controllo o le indicazioni comportamentali fornite;
- predisposizione di adeguati strumenti organizzativi e normativi atti a prevenire e/o impedire la realizzazione dei reati previsti dagli articoli *25-bis* e *25-bis. 1* del decreto 231 da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;
- predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dagli articolo *25-bis* del decreto.

Nell'espletamento delle rispettive attività e funzioni, oltre alle regole definite nel modello e nei suoi protocolli, gli organi sociali, gli amministratori, i dipendenti e i procuratori della società nonché i collaboratori e tutte le altre controparti contrattuali coinvolte nelle svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui agli articoli *25-bis* e *25-bis. 1*, al rispetto delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici delle aree a rischio identificate, tra i quali, ad esempio:

- svolgimento di verifiche sui diritti di terzi preesistenti al fine di garantire che non esistano già marchi uguali o simili depositati/registratori (ricerca di anteriorità) e che non vengano violati i diritti di terzi;
- definizione di apposite procure per la gestione ed il deposito dei marchi;
- svolgimento di specifiche analisi di sorveglianza brevettuale della concorrenza e attività di ricerca;
- attuazione di specifici controlli sui prodotti e sui relativi imballi (dall'analisi della composizione del prodotto fino al monitoraggio dell'ambiente della linea di produzione), finalizzati a garantire la qualità, la sicurezza e l'integrità dei prodotti e delle relative confezioni;
- predisposizione delle dichiarazioni di conformità dei prodotti;
- presenza di uno specifico processo di validazione delle etichette dei prodotti;
- svolgimento di specifici audit presso i propri fornitori al fine di verificare l'adeguatezza dei sistemi utilizzati per la produzione ed il rispetto delle norme previste dalla legge;
- presenza di uno specifico processo di gestione dei reclami;
- svolgimento di apposite verifiche sulle quantità in ingresso, sulla qualità di stoccaggio (in termini di temperatura e umidità), sulla preparazione delle consegne in ambienti controllati e sulle quantità caricate sui camioncini, al fine di evitare che vengano distribuiti prodotti alimentari con segni distintivi mendaci o non genuini;

- attuazione di specifiche verifiche sui contenuti delle comunicazioni pubblicitarie al fine di garantire la coerenza degli stessi rispetto alle caratteristiche del prodotto (i messaggi non devono, infatti, essere in alcun modo ingannevoli);
- presenza di uno specifico processo di gestione delle attività di raccolta e archiviazione della documentazione relativa ai prodotti;
- definizione di apposite procure per l'assicurazione della qualità e dell'igiene dei prodotti alimentari e per l'assicurazione della conformità a legge dei prodotti alimentari e delle materie prime;
- previsione di procedure aziendali relative al sistema di gestione della qualità;
- erogazione di specifici corsi di formazione sugli aspetti nutrizionali del prodotto e sulle tematiche inerenti la qualità e l'igiene dei prodotti alimentari;
- presenza di uno specifico processo di gestione delle contestazioni.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Aree a rischio reato - Attività sensibili	Controlli preventivi
Realizzazione e sviluppo di nuovi prodotti, soluzioni, tecnologie e strumenti, anche di imballaggio	<p>Gestione dell'<i>Intellectual Property</i> e portafoglio marchi: con riferimento a invenzioni, informazioni segrete, marchi ed altri segni distintivi, disegni e modelli, modelli di utilità, indicazioni geografiche, denominazioni di origine e altre privative industriali nazionali o estere, deve essere adottato e attuato uno strumento normativo e/o organizzativo che:</p> <ul style="list-style-type: none"> • preveda la coerenza delle attività di gestione <i>dell'Intellectual Property</i> e del portafoglio marchi rispetto alle disposizioni di legge vigenti in materia; • definisca principi, attività, ruoli e responsabilità in relazione allo sviluppo, gestione, protezione e valorizzazione <i>dell'Intellectual Property</i> e del portafoglio marchi; • definisca le modalità operative connesse alla protezione <i>dell'Intellectual Property</i> e del portafoglio marchi (che comprenda, tra l'altro, la verifica della sussistenza dei requisiti di brevettabilità <i>dell'Intellectual Property</i> o di registrazione dei marchi); • definisca le modalità operative in merito alle attività di concessione di licenze d'uso (<i>in and out</i>) nonché di acquisto e/o cessione di <i>Intellectual Property</i> e marchi.

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 41 di 85
------------------------------	---------------------	-----------------	--------------------

Acquisizione, rivendica, registrazione e gestione di marchi, brevetti, disegni,	Acquisto prodotti/opere tutelate da proprietà intellettuale/industriale. È consigliabile adottare ed attuare uno strumento normativo e organizzativo che, nell'ambito dell'acquisizione di prodotti /opere tutelati da diritti di proprietà
---	--

<p>modelli o altri titoli o diritti di proprietà industriale</p>	<p>industriale/ intellettuale, preveda il coinvolgimento della competente funzione legale nella definizione, qualora applicabile, di clausole contrattuali contenenti l'impegno/attestazione (a seconda dei casi) della controparte: di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni, modelli od opere tutelate dal diritto d'autore oggetto di cessione ovvero di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;</p> <p>che i diritti di utilizzo e/o di sfruttamento delle privative industriali e/o intellettuali, oggetto di cessione o di concessione in uso, non violano alcun diritto di proprietà industriale/ intellettuale in capo a terzi;</p> <p>a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio dovesse derivarle per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.</p>
<p>Partecipazione a procedure di cui al punto precedente in associazione con altri partner (RTI, ATI, <i>joint venture</i>, consorzi, etc.).</p>	<p>Per evitare la propagazione di responsabilità agli enti che abbiano realizzato forme di associazione con altri partner commerciali, a fronte di un illecito corruttivo commesso dall'esponente di uno di questi ultimi, può essere utile: la previsione di un omogeneo approccio e di una condivisa sensibilità da parte dei componenti dell'ATI/RTI o dei consorziati o intermediari sui temi afferenti la corretta applicazione del decreto 231, anche in relazione all'adozione di un proprio modello organizzativo da parte di ciascun componente del raggruppamento nonché all'impegno, esteso a tutti i soggetti coinvolti, di adottare un proprio Codice Etico;</p> <p>acquisizione dai partner di informazioni sul sistema dei presidi dagli stessi implementato, nonché flussi di informazione tesi ad alimentare un monitoraggio gestionale, ovvero attestazioni periodiche sigli ambiti di rilevanza 231 di interesse (es. attestazioni rilasciate con cadenza periodica in cui ciascun partner dichiara di non essere a conoscenza di informazioni o situazioni che possano, direttamente o indirettamente, configurare le ipotesi di reato previste dal decreto 231);</p> <p>eventuale definizione di specifiche clausole contrattuali di audit (da svolgere sia con idonee strutture presenti all'interno dell'aggregazione tra imprese che con l'eventuale ricorso a soggetti esterni), da attivarsi a fronte di eventuali indicatori di rischio rilevati;</p> <p>adozione, accanto al Codice Etico rispetto al quale si pone in rapporto sinergico, di uno specifico Codice di Comportamento rivolto ai fornitori e partner che contenga le regole etico-sociali destinate a disciplinare i rapporti dei suddetti soggetti con l'impresa, cui auspicabilmente aderiscano le controparti che affiancano la società nelle diverse opportunità di business (es. nell'ambito di <i>joint ventures</i>, ATI, RTI, consorzi, etc.).</p>
<p>Acquisto e cessione di beni o servizi</p>	<p>Rapporti con fornitori e controparti contrattuali: occorre adottare e attuare uno strumento normativo o organizzativo che definisca modalità di qualifica, valutazione e classificazione dei fornitori e dei contrattisti. In</p>

particolare tale strumento dovrebbe: definire ruoli, responsabilità e modalità di effettuazione della qualifica/valutazione/classificazione⁴;

in caso di appalto, prevedere che si tenga conto oltre che dei requisiti di carattere generale e morale⁵ degli appaltatori, anche dei requisiti tecnico-professionali, ivi incluse le necessarie autorizzazioni previste dalla normativa ambientale e di salute e sicurezza;

prevedere che si tenga conto della rispondenza di quanto eventualmente fornito con le specifiche di acquisto e con le migliori tecnologie disponibili in tema di tutela dell'ambiente, della salute e della sicurezza.

⁴ In merito alla valutazione/classificazione dei fornitori, il primo punto dello standard di controllo si considera rispettato qualora sia adottato e attuato uno strumento normativo che definisca classi omogenee di fornitori/operatori "valutati/classificati" d'ufficio.

⁵ I requisiti di carattere generale, morale e tecnico-professionali devono essere valutati anche con riferimento a eventuali subappaltatori.

Art. 25-ter d.lgs. 231/2001 - Reati societari

Reati presupposto		
Codice civile	art. 2621	False comunicazioni sociali
	art. 2622	False comunicazioni sociali in danno della società, dei soci o dei creditori
	art. 2625	Impedito controllo
	art. 2626	Indebita restituzione dei conferimenti
	art. 2627	Illegale ripartizione degli utili e delle riserve
	art. 2628	Illecite operazioni sulle azioni o quote sociali o della società controllante
	art. 2629	Operazioni in pregiudizio dei creditori
	art. 2629-bis	Omessa comunicazione del conflitto di interessi
	art. 2632	Formazione fittizia del capitale
	art. 2633	Indebita ripartizione dei beni sociali da parte dei liquidatori
	art. 2635	Corruzione tra privati
	art. 2636	Illecita influenza sull'assemblea
	art. 2637	Aggiotaggio
	art. 2638	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza
d.lgs. 58/1998	art. 173-bis	Falso in prospetto
d.lgs. 39/2010	art. 27	Falsità nelle relazioni o nelle comunicazioni delle società di revisione

1. CONSIDERAZIONI GENERALI

Il d.lgs. n. 61/2002 ha previsto l'inserimento nel decreto 231 di specifiche sanzioni a carico dell'ente *"in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica"*.

La predisposizione di un modello di organizzazione, gestione e controllo e di un Organismo di Vigilanza dotato di poteri effettivi, oltre ad assumere un'importante valenza probatoria della volontà dell'ente di eliminare i difetti di organizzazione che possano facilitare la commissione di determinati illeciti, può assicurare un'accresciuta trasparenza delle procedure e dei processi interni all'impresa e, quindi, maggiori possibilità di controllo dell'operato dei *manager*.

Gli atti parlamentari relativi al decreto 61 infatti chiarivano: *"Appare positivo, ai fini preventivi, che i soci sappiano che almeno parte del loro investimento può essere eroso dalla condotta illecita dei manager, stimolando così l'attività di controllo; ma lo stesso circolo virtuoso, può riferirsi anche alla struttura cui è affidata la gestione, che dovrebbe essere sollecitata ad intraprendere le azioni necessarie per evitare che si creino condizioni favorevoli alla commissione di reati. [...] Questa pressione sui vertici della società giustifica anche la previsione di una responsabilità in capo alla società nei casi in cui il reato sia stato commesso da soggetti non apicali, ma avrebbe potuto essere impedito da un'adeguata e doverosa vigilanza dei soggetti sovraordinati"*.

Per quanto riguarda il profilo strettamente sanzionatorio, inoltre, è importante sottolineare che la legge di riforma del risparmio (L. n. 262/2005) ha realizzato un inasprimento generalizzato delle pene pecuniarie applicabili agli enti per la commissione di reati societari, raddoppiandone i relativi importi. L'art. 39, co. 5, della legge 262/2005 dispone, infatti, che *"Le sanzioni pecuniarie previste dall'articolo 25-ter del decreto legislativo 8 giugno 2001, n. 231, sono raddoppiate"*.

Da ciò nasce dunque la duplice esigenza di: a) approntare specifiche misure organizzative e procedurali - nell'ambito del modello già delineato nelle Linee Guida per i reati contro la PA - atte a fornire ragionevole garanzia di prevenzione di questa tipologia di reati; b) precisare i compiti principali dell'Organismo di Vigilanza per assicurare l'effettivo, efficace, efficiente e continuo funzionamento del modello stesso.

Specificità proprie dei reati societari

I reati societari possono qualificarsi come propri perché soggetti attivi possono essere solo *"amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza"*. Tale caratteristica ripropone le questioni relative all'autonomia, alla collocazione nell'organizzazione aziendale, ai poteri e alla comunicazione da e verso l'Organismo di Vigilanza già affrontate nel relativo capitolo.

Le linee direttrici della legge delega sulla riforma del diritto societario (l. n. 366/2001), che propongono in tema di organizzazione interna delle società per azioni alcune impostazioni tipiche di ordinamenti stranieri, contengono importanti spunti di riferimento utili per risolvere le predette questioni, almeno riguardo alle società per azioni o, comunque, a struttura organizzativa complessa.

In particolare, è opportuno richiamare due dei tre modelli previsti all'articolo 4, comma 8, lettera *d*), della legge delega n. 366/2001:

- il modello tedesco, che prevede la presenza di un Consiglio di Gestione, con compiti amministrativi, ed un Consiglio di Sorveglianza, eletto dall'assemblea e sovraordinato al Consiglio di Gestione, di cui nomina i componenti e sorveglia l'attività;
- il modello anglosassone, che si basa su un Consiglio di Amministrazione al cui interno è costituito un Comitato di Controllo, formato in prevalenza da soggetti non coinvolti nella gestione dell'azienda.

Questi modelli, più di quello tradizionale attualmente previsto dal codice civile (CdA/Collegio Sindacale), potrebbero garantire:

- autonomia ed indipendenza, per la posizione istituzionale dell'Organo di Vigilanza, nonché per le sue modalità elettive;
- prontezza ed efficacia negli adempimenti comunicativi sia verticali sia orizzontali. L'Organismo di Vigilanza, in virtù della sua collocazione, può utilizzare i tradizionali percorsi di comunicazione disciplinati dal codice civile, ma anche acquisire direttamente informazioni dal basso verso l'alto attraverso eventuali diramazioni dello stesso organismo all'interno dell'organizzazione aziendale;
- potere disciplinare: elemento naturalmente e spontaneamente collegato ai primi due.

Per quanto riguarda le società a responsabilità limitata, in assenza di specifiche indicazioni, non resta che muoversi analogamente e coerentemente a quanto sopra descritto prospettando, nell'ambito dell'autonomia statutaria, la costituzione di un organo ancora una volta distinto da quello di gestione, con carattere di autonomia e potere d'intervento sanzionatorio/disciplinare.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Modalità di realizzazione del reato - attività a rischio reato	Controlli preventivi
<p>False comunicazioni sociali - falso in prospetto</p> <p>Redazione del bilancio, delle relazioni o delle comunicazioni sociali previste dalla legge e, più in generale, di qualunque documento giuridicamente rilevante nel quale si evidenzino elementi economici, patrimoniali e finanziari dell'impresa, ancorché relativi al gruppo al quale essa appartiene o alle sue partecipazioni.</p>	<p>Inserimento nel Codice etico di specifiche previsioni riguardanti il corretto comportamento di tutti i dipendenti coinvolti nelle attività di formazione del bilancio o di altri documenti simili, così da garantire:</p> <ul style="list-style-type: none"> • massima collaborazione; • completezza e chiarezza delle informazioni fornite; • accuratezza dei dati e delle elaborazioni; • tempestiva segnalazione di eventuali conflitti di interesse. <p>Attività di formazione di base verso tutti i responsabili di funzione, affinché conoscano almeno le principali nozioni sul bilancio (norme di legge, sanzioni, principi contabili, ecc.)</p>

Istituzione di una procedura chiara e tempificata rivolta alle stesse funzioni di cui sopra, con cui si stabilisca quali dati e notizie debbono essere forniti all'Amministrazione, nonché quali controlli devono essere svolti su elementi forniti dall'Amministrazione e da "validare".

Previsione per il responsabile di funzione che fornisce dati ed informazioni relative al bilancio o ad altre comunicazioni sociali dell'obbligo di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse. Nella dichiarazione andrà di volta in volta asseverato ciò che obiettivamente e concretamente il soggetto responsabile può documentalmente dimostrare (anche a seguito di verifica successiva) sulla base dei dati in suo possesso, evitando, nell'interesse stesso dell'efficacia dei protocolli, affermazioni generali e generiche. Ciò anche al fine di evidenziare la necessità che i protocolli disciplinino efficacemente e conseguentemente responsabilizzino tutti i singoli passaggi di un procedimento che generalmente solo nella sua conclusione incontra un soggetto qualificabile come "Responsabile di funzione".

Se il bilancio della società è assoggettato a revisione e certificazione, è consigliabile:

- consegnare a tutti i componenti del Consiglio di amministrazione - in particolare dei membri del Comitato per il controllo e rischi, ove esistente - prima della riunione del Consiglio per l'approvazione dello stesso di:

bozza del bilancio, allegando una documentata certificazione dell'avvenuta consegna della bozza in questione;

giudizio sul bilancio (o attestazione similare, sufficientemente chiara ed analitica) da parte della società di certificazione, ove esistente;

lettera di attestazione o di manleva richiesta dalla società di revisione, ove esistente, sottoscritta dal massimo vertice esecutivo e siglata dal Responsabile amministrativo.

- prevedere almeno una riunione tra la società di certificazione, il

	<p>Collegio Sindacale, il Comitato per il controllo e rischi (ove esistente) e l'Organismo di Vigilanza prima della seduta del Consiglio di Amministrazione indetta per l'approvazione del bilancio, che abbia per oggetto tale documento, da documentarsi mediante verbale.</p> <ul style="list-style-type: none"> • comunicare sistematicamente all'Organismo di Vigilanza: incarichi conferiti, o che si intende conferire, alla società di revisione (se esistente) o a società ad essa collegate, diverso da quello concernente la certificazione del bilancio; copia delle comunicazioni alla Consob relative all'insussistenza di cause di incompatibilità tra la società di revisione e la società certificata valutazioni in ordine alla scelta della società di revisione (in base ad elementi quali professionalità, esperienza nel settore non solo in base all'economicità). <p>Invece, per le società il cui bilancio non è assoggettato a revisione e certificazione, si suggerisce di prevedere:</p> <ul style="list-style-type: none"> • uno o più incontri tra l'Organismo di Vigilanza e il Responsabile amministrativo, focalizzati sul bilancio, con eventuali approfondimenti ed analisi documentali di fattispecie di particolare rilievo e complessità presenti nella bozza predisposta, curando la stesura del relativo verbale firmato da entrambi; • almeno un incontro all'anno, in prossimità della riunione del Consiglio di Amministrazione, tra Organismo di Vigilanza e Collegio sindacale avente per oggetto il bilancio (con relativa nota integrativa), con redazione di verbale.
<p>Impedito controllo Gli amministratori di una società a fronte di una puntuale richiesta da parte del Collegio Sindacale in ordine al rispetto, da parte della società, di una determinata normativa, tengono una condotta non corretta e trasparente. In particolare, non assecondano la richiesta di informazioni da parte del Collegio sindacale mediante l'occultamento, anche accompagnato da artifici, della documentazione utile a</p>	<p>Esistenza di un sistema definito di responsabilità del vertice aziendale e di deleghe coerenti anche in tema di disciplina di <i>Corporate Governance</i>. Istituzione di riunioni periodiche tra Collegio Sindacale, Comitato di controllo e rischi (se esistente) ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/<i>Corporate Governance</i>, nonché il rispetto dei comportamenti</p>

<p>rappresentare i processi applicativi in sede aziendale di tale legge oppure l'esibizione parziale o alterata di detta documentazione. Perché tale condotta costituisca illecito ai sensi del decreto 231 deve derivare da essa un danno per la società.</p>	<p>conseguenti da parte degli Amministratori, del <i>management</i> e dei dipendenti.</p> <p>Riporto periodico al Vertice sullo stato dei rapporti con il Collegio Sindacale e le altre Autorità abilitate ai controlli sulla Società.</p>
<p>Omessa comunicazione del conflitto di interessi</p> <p>L'amministratore delegato di una società quotata non dichiara volutamente al Consiglio di Amministrazione l'interesse personale suo o di suoi familiari in una determinata operazione all'esame del Consiglio di amministrazione.</p>	<p>Esistenza di un sistema definito di responsabilità del Vertice aziendale e di deleghe coerenti con esso anche in tema di disciplina di <i>Corporate Governace</i>.</p> <p>Identificazione delle principali fattispecie di interessi degli amministratori.</p> <p>Procedure autorizzative per operazioni esposte a situazioni di conflitto di interesse evidenziate da singoli amministratori.</p>
<p>Illecita influenza sull'assemblea</p> <p>L'Amministratore delegato predispone apposita documentazione falsa o comunque alterata ai fini della deliberazione dell'assemblea su uno specifico ordine del giorno. Tale documentazione è in grado di influenzare la maggioranza dei soci e consente di soddisfare interessi economico-finanziari dell'Amministratore medesimo o di terzi. Resta fermo (anche secondo la giurisprudenza consolidata) che il reato non si verifica allorché - anche in assenza di una condotta illecita dell'Amministratore - la maggioranza sarebbe stata ugualmente raggiunta.</p>	<p>Istituzione di riunioni periodiche tra Collegio Sindacale, Comitato per il controllo e rischi (se esistente) ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/<i>Corporate Governance</i> (compresa quella in tema di "parti correlate"), nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del <i>management</i>, dei dipendenti.</p>
<p>Aggiotaggio</p> <p>Gli amministratori e i dipendenti di una società diffondono notizie false sulla società medesima (ad esempio, dati economico-finanziari o dati relativi a situazioni interenti alla gestione di tale società), che, come tali, sono in grado di determinare una sensibile alterazione del prezzo riguardante il titolo azionario di detta società. Tale condotta beneficia lo stesso dipendente e/o terzi grazie a transazioni speculative tempestivamente operate dai medesimi in sede di compravendita di detto titolo azionario.</p>	<p>Istituzione di riunioni periodiche tra Collegio Sindacale, Comitato per il controllo e rischi (se esistente) ed Organismo di Vigilanza per verificare l'osservanza della disciplina prevista in tema di normativa societaria/<i>Corporate Governance</i>, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del Management e dei dipendenti.</p> <p>Procedure autorizzative per comunicati stampa, che prevedano controlli incrociati sulle successive bozze dei comunicati e fino alla versione definitiva, attraverso il coinvolgimento delle strutture responsabili e dei soggetti preposti alle verifiche contabili.</p> <p>Procedure autorizzative per acquisti e vendite di azioni proprie e/o di altre società.</p>

<p>Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza Gli Amministratori di società quotate in borsa trasmettono alla Consob il progetto di bilancio con relazioni e allegati, riportando notizie false o comunque notizie incomplete e frammentarie - anche mediante formulazioni generiche, confuse e/o imprecise - relativamente a determinate rilevanti operazioni sociali al fine di evitare possibili controlli da parte della Consob (ad esempio in tema di acquisizione di "partecipazioni rilevanti" in altre società per azioni non quotate).</p>	<p>Introduzione/integrazione dei principi di disciplina (regolamenti/procedure) in tema di rapporti di <i>Corporate Governance</i> e di osservanza della normativa societaria. Istituzione di riunioni periodiche tra Collegio Sindacale, Comitato per il controllo e rischi (se esistente) ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/<i>Corporate Governance</i>, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del Management e dei dipendenti. Previsione di apposito sistema sanzionatorio interno aziendale. Report periodici al vertice aziendale sullo stato dei rapporti con le Autorità pubbliche di Vigilanza.</p>
<p>Illecite operazioni sulle azioni o quote sociali o della società controllante L'amministratore dà a un terzo l'incarico di acquistare e/o sottoscrivere azioni in nome proprio e per conto della società. Operazioni in pregiudizio dei creditori Violazione delle disposizioni che presiedono al corretto svolgimento delle operazioni di riduzione del capitale sociale, fusione e scissione societaria, sorretta dalla volontà (anche come mera accettazione del rischio) di verifica di un danno per i creditori</p>	<p>Programma di informazione/formazione periodica degli amministratori, del management e dei dipendenti sulla normativa di <i>Corporate Governance</i> e sui reati/illeciti amministrativi in materia societaria. Istituzione di riunioni periodiche tra Collegio Sindacale, Comitato per il controllo e rischi (se esistente) ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/<i>Corporate Governance</i>. Procedure di: autorizzazione dell'acquisto di azioni o quote proprie e/o della società controllante; di disciplina delle operazioni di riduzione del capitale sociale, fusione e scissione societaria.</p>
<p>Corruzione tra privati Costituiscono aree a rischio reato: • la predisposizione di bandi di gara/partecipazione a procedure competitive</p>	<p>Nella negoziazione e stipula di contratti attivi⁶, devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della negoziazione e stipula di contratti attivi prevedano:</p>

⁶ Vedi nota 7.

finalizzati alla negoziazione o stipula di contratti attivi, cioè in grado di generare un ricavo per la società;

- la negoziazione, stipula e gestione di contratti attivi con società, consorzi, fondazioni associazioni e altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa;
- gestione delle attività di *trading* su *commodities*, finanziario o fisico: selezione delle controparti e dei prodotti, gestione dei *deals*, stipula dei contratti;
- gestione dei rapporti con società, consorzi, fondazioni associazioni e altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa, dal cui mancato svolgimento possa derivare un vantaggio per la società o per le quali la stessa possa avere un interesse (per esempio, analisti finanziari, *mass media*, agenzie di *rating*, organismi di certificazione e di valutazione di conformità, etc.);
- selezione dei fornitori di beni e servizi, negoziazione e stipula dei relativi contratti;
- gestione di contratti per l'acquisto di beni e servizi.

Come esempi di dettaglio, può menzionarsi la corresponsione di una somma di denaro o altra utilità (quale ad esempio un regalo di non modesto valore o di ospitalità oltre i criteri di ragionevolezza e di cortesia commerciale):

dal Direttore Commerciale (o suo sottoposto) al responsabile degli acquisti di una società cliente per favorire i prodotti aziendali rispetto a quelli di migliore qualità o con migliore rapporto qualità/prezzo di un concorrente;

da un soggetto aziendale all'Amministratore Delegato (o al Direttore Generale) di una società concorrente affinché questi ignori una opportunità d'affari nella quale l'impresa per cui il corruttore lavora ha un proprio interesse;

da un addetto alla Ricerca & Sviluppo al Direttore R&D di società concorrente al fine di farsi rivelare segreti industriali quali informazioni segrete o invenzioni non ancora brevettate;

dall'Amministratore Delegato di una società al sindaco di una società

- *l' iter di* definizione e attuazione delle politiche commerciali;
- le modalità ed i parametri per la determinazione del prezzo e della congruità dello stesso rispetto ai riferimenti di mercato, tenuto conto dell'oggetto del contratto e delle quantità;
- previsioni contrattuali standardizzate in relazione alla natura e tipologia di contratto, ivi incluse previsioni contrattuali finalizzate all'osservanza di principi di controllo/regole etiche nella gestione delle attività da parte del terzo, e le attività da seguirsi in caso di eventuali scostamenti;
- l'approvazione del contratto da parte di adeguati livelli autorizzativi.

Nella gestione di contratti attivi devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della gestione dei contratti attivi prevedano:

- in caso di contratto aperto, la verifica della coerenza dell'ordine rispetto ai parametri previsti nel contratto medesimo;
- la verifica della completezza ed accuratezza della fattura rispetto al contenuto del contratto/ordine, nonché rispetto ai beni/servizi prestati;
- ove applicabile, la verifica - anche a campione - della conformità della fatturazione alle prescrizioni di legge;
- i criteri e le modalità per l'emissione di note di debito e note di credito.

Nella gestione delle operazioni di *trading* devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito del *trading* di petrolio, prodotti petroliferi, gas, energia elettrica, certificati verdi, derivati prevedano:

- le modalità di accreditamento delle controparti finanziarie;
- la verifica della presenza della controparte nell'elenco delle controparti finanziarie accreditate;
- la definizione di limiti di rischio per le operazioni di *trading*;
- la definizione delle tipologie di *commodities/prodotti* derivati che possono essere oggetto delle transazioni e le modalità per la relativa

terza quotata per carpire in anticipo rispetto al mercato informazioni sensibili e favorirne così la acquisizione del pacchetto di controllo da parte della società di appartenenza.

da un soggetto aziendale al liquidatore di una società per favorire l'acquisto a valore inferiore al mercato di un bene della società in liquidazione o per transigere un debito a valore inferiore a quello reale.

dall'Amministratore Delegato della società controllante al dirigente preposto alla redazione dei documenti contabili societari della società controllata, affinché rilasci una attestazione di attendibilità del bilancio non conforme al vero con riferimento ad una operazione infragruppo a danno della controllata ed a vantaggio della controllante.

autorizzazione;

- l'autorizzazione della transazione nel rispetto dei relativi limiti di rischio;
- lo svolgimento di una verifica successiva all'operazione sull'allineamento dei prezzi praticati rispetto ai prezzi di mercato;
- la verifica della completezza ed accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto nonché rispetto alla transazione effettuata.

Nei rapporti con società, consorzi, fondazioni, associazioni ed altri enti privati, devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgano attività professionali/istituzionali o di impresa dal cui svolgimento o mancato svolgimento possa derivare un vantaggio per la società o per le quali la stessa possa avere un interesse prevedano:

- l'individuazione delle tipologie di rapporti e le relative modalità di gestione;
- le modalità di raccolta, verifica e approvazione della documentazione da trasmettere agli esponenti di società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgano attività professionale e di impresa per le quali l'ente abbia un interesse o dalle quali possa derivare un vantaggio, con il supporto delle funzioni competenti.

Inserimento nel Codice etico di specifiche previsioni riguardanti il corretto comportamento di tutti i dipendenti coinvolti in rapporti con società concorrenti o target (ad. es., rispetto delle regole di corretta concorrenza; trasparenza e tracciabilità dei comportamenti; divieto di regalie o promesse di benefici).

Attività di formazione di base verso tutti i responsabili di funzione, particolarmente dell'area commerciale, ricerca e sviluppo, progetti speciali e dell'alta dirigenza, affinché conoscano le principali nozioni in tema di reato di corruzione privata (in particolare norme di legge, sanzioni, fattispecie a rischio reato).

	<p>Istituzione di una procedura volta a fornire ai soggetti aziendali alcune regole comportamentali da seguire nella gestione di rapporti con professionisti e soggetti appartenenti a società terze, che preveda:</p> <ul style="list-style-type: none"> • la segnalazione tempestiva ai superiori e all'Organismo di Vigilanza aziendale di ogni richiesta di denaro o di regalia non giustificata dai normali rapporti amministrativi, ricevuta da soggetti appartenenti ad altre aziende; • nell'ambito della procedura che precede (o mediante autonomo protocollo) prevedere regole predefinite per il conferimento di incarichi o consulenze a soggetti terzi, ispirandosi a criteri di legalità, trasparenza, condivisione funzionale, inerenza e giustificabilità. <p>Istituzione di una procedura per il controllo dei flussi finanziari e la tracciabilità dei pagamenti.</p> <p>Previsione di un meccanismo di segnalazione tempestiva ai superiori di qualsiasi situazione di conflitto di interessi che possa insorgere in capo a soggetti aziendali e relative modalità di intervento.</p> <p>Istituzione di una procedura che garantisca il rispetto dei criteri di legalità, trasparenza, condivisione funzionale e giustificabilità nel:</p> <ul style="list-style-type: none"> • regolare la gestione della proprietà industriale ed intellettuale e di un protocollo volto a regolare la acquisizione alla società di invenzioni o soluzioni innovative individuate o sviluppate da soggetti terzi; • disciplinare il rapporto con soggetti appartenenti a società concorrenti, clienti o <i>target</i>.
Selezione, assunzione e gestione amministrativa del personale.	<p>Adozione di uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione, assunzione e gestione amministrativa del personale prevedano:</p> <ul style="list-style-type: none"> • un processo di pianificazione delle risorse da assumere che tenga conto del fabbisogno; • l'individuazione dei requisiti minimi necessari (profilo) per ricoprire il ruolo e il relativo livello di retribuzione nel rispetto di quanto previsto dai

Contratti Collettivi Nazionali del Lavoro (ove applicabili) ed in coerenza con le tabelle retributive di riferimento;

- la definizione di un processo di selezione del personale che disciplini:
 - la ricerca di una pluralità di candidature in funzione della complessità del ruolo da ricoprire;
 - la gestione dei conflitti di interesse tra il selezionatore e il candidato;
 - la verifica, attraverso diverse fasi di screening, della coerenza delle candidature con il profilo definito;
- lo svolgimento di verifiche pre-assuntive, anche eventualmente nel rispetto di eventuali legislazioni estere rilevanti nel caso di specie) finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che esponano la società al rischio di commissione di reati presupposto in tema di responsabilità dell'ente (con particolare attenzione all'esistenza di procedimenti penali/carichi pendenti, di conflitto di interesse/relazioni tali da interferire con le funzioni di pubblici ufficiali, incaricati di pubblico servizio chiamati ad operare in relazione ad attività per le quali la società ha un interesse concreto così come con rappresentanti di vertice di società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa che abbiano un particolare rilievo ai fini aziendali);
- la definizione di eventuali circostanze ostative nonché delle diverse circostanze che si pongono solo come punto di attenzione all'assunzione a seguito del completamento delle verifiche pre-assuntive;
- l'autorizzazione all'assunzione da parte di adeguati livelli;
- le modalità di apertura e di gestione dell'anagrafica dipendenti;
- sistemi, anche automatizzati, che garantiscano la tracciabilità della rilevazione delle presenze in accordo con le previsioni di legge applicabili;
- la verifica della correttezza delle retribuzioni erogate.

Previsione di procedure di autorizzazione delle richieste di acquisto e di:

Approvvigionamento di beni, lavori e servizi.

- criteri e modalità di assegnazione del contratto;
- ricorso alla procedura di assegnazione diretta solo per casi limitati e chiaramente individuati, adeguatamente motivati e documentati, nonché sottoposti a idonei sistemi di controllo e sistemi autorizzativi a un adeguato livello gerarchico;
- modalità e criteri per la predisposizione e l'approvazione del bando di gara, nonché per la definizione e approvazione di *short vendor list*;
- un modello di valutazione delle offerte (tecniche/economiche) informato alla trasparenza e a criteri il più possibile oggettivi;
- previsioni contrattuali standardizzate in relazione a natura e tipologie di contratto, contemplando clausole contrattuali finalizzate all'osservanza di principi di controllo nella gestione delle attività da parte del terzo e le attività da seguirsi nel caso di eventuali scostamenti.

Art. 25-quater d.lgs. 231/2001 - Delitti con finalità di terrorismo o di eversione dell'ordine democratico

1. CONSIDERAZIONI GENERALI

La legge 14 gennaio 2003, n. 7, di ratifica ed esecuzione della Convenzione internazionale firmata a New York per la repressione del finanziamento del terrorismo del 1999, introduce nel decreto 231 l'art. 25-quater.

Ai sensi di tale norma, costituiscono reato presupposto di tale illecito tutti i delitti con finalità di terrorismo o eversione dell'ordine democratico previsti dal codice penale e dalla legislazione complementare, nonché i delitti diversi da questi ultimi ma posti in essere in violazione di quanto stabilito dall'art. 2 della Convenzione di New York.

Tra le fattispecie previste dal codice penale, le più rilevanti sono le seguenti: associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis c.p.); assistenza agli associati (art. 270-ter c.p.); arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c.p.); addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.); condotte con finalità di terrorismo (art. 270-sexies c.p.); attentato per finalità terroristiche o di eversione (art. 280 c.p.); atto di terrorismo con ordigni micidiali o esplosivi (art. 280-bis c.p.); sequestro di persona a scopo di terrorismo o di eversione (art. 289-bis c.p.); istigazione a commettere uno dei delitti contro la personalità dello Stato (art. 302 c.p.).

Questi ultimi sono i reati diretti a fornire direttamente o indirettamente fondi a favore di soggetti che intendano porre in essere reati di terrorismo. In particolare, la Convenzione rinvia ai reati previsti da altre convenzioni internazionali, tra i quali: il dirottamento di aeromobili, gli attentati contro personale diplomatico, il sequestro di ostaggi, l'illecita realizzazione di ordigni nucleari, i dirottamenti di navi, l'esplosione di ordigni, ecc.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Aree/settori a rischio reato	Controlli preventivi
Settore finanziario. Settore assicurativo.	Specifiche previsioni del codice etico. Diffusione del codice etico verso tutti i dipendenti. Programma di informazione/formazione periodica dei dipendenti delle aree a rischio. Controllo dei flussi finanziari aziendali. Controllo della documentazione aziendale.

Art. 25-quater.1 d.lgs. 231/2001 - Pratiche di mutilazione degli organi genitali femminili

La Legge n. 7 del 9 gennaio 2006, contenente disposizioni in materia di prevenzione e divieto delle pratiche di infibulazione, ha introdotto nel codice penale il reato di pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p., successivamente modificato e integrato) e ha esteso a tale reato l'ambito di applicazione del d. lgs. n. 231/2001 (art. 25-quater. 1). La *ratio* della norma è di sanzionare enti e strutture (in particolare, strutture sanitarie, organizzazioni di volontariato, ecc.) che si rendano responsabili della realizzazione, al loro interno, di pratiche mutilative vietate.

In particolare, all'ente nella cui struttura viene commesso il delitto di cui all'art. 583-bis c.p. sono applicabili la sanzione pecuniaria da 300 a 700 quote e le sanzioni interdittive per una durata minima di un anno. Inoltre, se l'ente interessato è un ente privato accreditato, è disposta la revoca dell'accreditamento. Infine, si prevede la sanzione dell'interdizione definitiva dall'esercizio dell'attività, se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo - unico o prevalente - di consentire o agevolare la commissione del reato (art. 16, co. 3, decreto 231).

Ai fini della prevenzione di questa fattispecie di reato, è opportuno inserire nel Codice etico specifici richiami volti a impedirne la commissione.

Art. 25-quinquies d.lgs. 231/2001 - Delitti contro la personalità individuale

La Legge n. 228/2003, recante misure contro la tratta di persone, ha introdotto nel decreto 231 l'art. 25-quinquies che prevede l'applicazione di sanzioni amministrative agli enti per la commissione di delitti contro la personalità individuale.

L'art. 25-quinquies è stato successivamente integrato dalla Legge n. 38/2006 contenente "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*", che modifica l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600-ter e 600-quater c.p.), includendo anche le ipotesi in cui tali illeciti sono commessi mediante l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori degli anni diciotto o parti di esse (cd. pedopornografia virtuale). Tale legge ha in parte modificato anche la disciplina dei delitti di prostituzione minorile, pornografia minorile e detenzione di materiale pornografico (artt. 600-bis, 600-ter e 600-quater c.p.), già rilevanti ai fini della responsabilità amministrativa degli enti.

La disciplina dei reati presupposto in esame è stata oggetto di diverse modifiche ad opera di successivi interventi normativi (v. Legge n. 108/2010; Legge n. 172/2012; d. lgs. n. 24/2014 e d. lgs. n. 39/2014). In particolare, si segnala che la legge n. 172/2012 (recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonche' norme di adeguamento dell'ordinamento interno*") ha introdotto nel codice penale il delitto di adescamento di minorenni (art. 609-undecies) che, in seguito, il d. lgs. n. 39/2014 ha inserito tra i reati presupposto previsti dall'art. 25-quinquies del decreto 231. Inoltre, il d. lgs. n. 24/2014 ha modificato le fattispecie di reato di cui agli artt. 600 e 601 del codice penale.

Ai fini della responsabilità dell'ente, mentre è difficile individuare la sussistenza dell'interesse o vantaggio dell'ente stesso nel caso di alcuni tra i delitti sopra richiamati (ad es. prostituzione minorile), l'ente può trarre beneficio da illeciti quali la pornografia minorile o le iniziative turistiche volte allo sfruttamento della prostituzione minorile,

Pertanto, le società che svolgono attività per via telematica (ad es. nei settori dell'editoria, della pubblicità, del commercio elettronico) risultano particolarmente esposte al rischio di verifica di tali reati e sono tenute ad analizzare con maggiore attenzione il contesto aziendale interno per individuare aree, processi e soggetti a rischio e predisporre un sistema di controlli idoneo a contrastare efficacemente tali rischi. Ciò soprattutto a seguito della legge n. 38/2006 che prevede la responsabilità dell'ente per i delitti di pornografia minorile e di detenzione di materiale pornografico commessi, nel suo interesse o a suo vantaggio, da persone in posizione apicale o subordinata, anche se relativi al materiale pornografico virtuale che ha ad oggetto minori.

Con particolare riferimento alla fattispecie delle iniziative turistiche per lo sfruttamento della prostituzione minorile, si tratta di un'ipotesi che potrebbe riguardare imprese operanti nel settore dell'organizzazione di viaggi che, pertanto, sono tenute a verificare quali sono le aree aziendali a rischio (ad esempio, produzione e distribuzione o gestione dei siti Internet) e a predisporre misure sanzionatorie nei confronti dei soggetti coinvolti negli illeciti rilevanti.

In relazione ai reati connessi alla schiavitù, tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie illecita, ma anche a chi consapevolmente agevola - anche solo sul piano finanziario - la medesima condotta. Al riguardo, la condotta rilevante è costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi. Per prevenire la commissione di tali reati l'ente può prevedere le misure indicate nella tabella che segue, in via esemplificativa.

Fattispecie incriminatrici	Controlli preventivi
Prostituzione e pornografia minorile, iniziative turistiche per sfruttamento prostituzione minorile	<p>Introduzione nel Codice etico di uno specifico divieto in tema di pornografia minorile. Strumenti informatici che impediscano accesso e/o ricezione di materiale relativo alla pornografia minorile. Richiami netti e inequivocabili a un corretto utilizzo degli strumenti informatici in possesso dei dipendenti.</p> <p>Ponderata valutazione e disciplina dell'organizzazione diretta e/o indiretta di viaggi o di periodi di permanenza in località estere con specifico riguardo a località note per il fenomeno del c.d. "turismo sessuale".</p> <p>Attenta valutazione di possibili partnership commerciali con società operanti in settori quali la comunicazione telematica di materiale relativo alla pornografia minorile e il turismo nelle aree geografiche richiamate al punto precedente.</p> <p>Sistema di sanzioni disciplinari adeguato alla peculiare gravità delle violazioni in esame.</p>
Reati connessi alla schiavitù	<p>Introduzione nel Codice etico di uno specifico impegno a rispettare - e a far rispettare ai propri fornitori - la normativa vigente in materia di lavoro, con particolare attenzione al lavoro minorile e al tema della salute e sicurezza.</p> <p>Diversificazione dei punti di controllo interni alla struttura aziendale preposta all'assunzione e gestione del personale.</p> <p>Previsione dello specifico impegno dei propri partner a rispettare gli obblighi di legge in tema di: tutela del lavoro minorile e delle donne; condizioni igienico-sanitarie e di sicurezza; diritti sindacali o di associazione e rappresentanza. Ai fini della verifica del rispetto di tale impegno, l'ente può prevedere visite ispettive presso i propri fornitori ovvero richiedere loro ogni documentazione utile.</p>

Art. 25-sexiesd.lgs. 231/2001 - Abusi di mercato

Reati presupposto		
T.U.F. (D.lgs. 58/1998)	art. 184	Abuso di informazioni privilegiate
	art. 185	Manipolazione di mercato

1. CONTESTO NORMATIVO DI RIFERIMENTO

L'art. 9 della legge n. 62/2005 (Legge Comunitaria per il 2004) ha recepito la direttiva 2003/6/CE del Parlamento europeo e del Consiglio del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (c.d. abusi di mercato) e ha introdotto l'art. 25-sexies nel decreto n. 231/2001, estendendo l'ambito della responsabilità amministrativa degli enti alle condotte che integrano tali abusi.

Il sistema sanzionatorio definito dalla Legge Comunitaria per i cd. abusi di mercato si estende oltre il profilo della responsabilità ai sensi del decreto 231. Infatti, esso prevede sanzioni amministrative a carico sia della persona fisica che della società per illeciti amministrativi, nonché sanzioni penali a carico della persona fisica e sanzioni amministrative a carico della società, nel caso in cui l'illecito assuma rilevanza penale.

La Legge Comunitaria interviene sia sul Codice Civile che sul Testo Unico dell'Intermediazione Finanziaria (d. lgs. n. 58/1998, cd. TUF).

Con riferimento al Codice Civile, viene modificato l'art. 2637 che, mentre prima sanzionava il reato di agiotaggio commesso in relazione a strumenti finanziari quotati e non quotati, oggisi applica ai soli casi di agiotaggio posti in essere rispetto a *"strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato"* Nel caso di strumenti finanziari quotati si applicano, invece, le norme del TUF.

Interventi più importanti hanno riguardato il TUF.

In primo luogo, è stato riscritto l'art. 114 relativo alle comunicazioni al pubblico, che obbliga gli emittenti quotati e i soggetti che li controllano a comunicare al pubblico, senza indugio, le informazioni privilegiate relative a detti emittenti o alle società da essi controllate. La definizione di informazioni privilegiate è contenuta nel nuovo art. 181 TUF, anch'esso modificato, ai sensi del quale *"per informazione privilegiata si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti"*

finanziari". I successivi commi specificano ulteriormente tale nozione. Al riguardo, la nozione di strumenti finanziari, utile a delimitare l'ambito di applicazione della normativa in esame, è contenuta nell'ari 180 TUF.

Inoltre, l'art. 114 TUF rinvia la definizione delle modalità della comunicazione alla Consob, che le ha stabilite nel Regolamento di attuazione del TUF, concernente la disciplina degli emittenti (c.d. Regolamento emittenti) e nel Regolamento di attuazione del TUF e del D. Lgs. n. 213/1998 in materia di mercati (c.d. Regolamento mercati). La norma rinvia altresì alla regolamentazione Consob la disciplina dei casi in cui i soggetti obbligati possano ritardare la comunicazione obbligatoria. Per l'inottemperanza all'obbligo di comunicazione è prevista una sanzione pecuniaria (art. 193 TUF).

Infine, l'art. 115-bis del TUF prevede che i soggetti obbligati alla comunicazione devono istituire e mantenere regolarmente aggiornato un registro delle persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, hanno accesso alle informazioni privilegiate.

Oltre all'obbligo di comunicazione delle informazioni privilegiate, la normativa in esame disciplina anche gli illeciti di abuso di informazioni privilegiate e manipolazione del mercato, prevedendo, come anticipato, sanzioni sia penali che amministrative.

In particolare, mentre gli artt. **184 e 185 TUF** disciplinano, rispettivamente, il reato di **abuso di informazioni privilegiate e di manipolazione del mercato**, gli artt. 187-bis e 187-ter TUF (introdotti dalla Legge Comunitaria) tipizzano, rispettivamente, gli illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione del mercato. Questi ultimi illeciti sono puniti - salve le relative sanzioni penali applicabili quando il fatto integra un reato - con sanzioni amministrative pecuniarie. Si evidenzia che, trattandosi di illeciti amministrativi, le sanzioni previste dal TUF si applicano anche quando le condotte richiamate sono poste in essere a titolo di mera colpa. Il potere di comminare tali sanzioni amministrative è affidato alla Consob dall'ari 187-ò/s.

Il sistema sanzionatorio, sul piano amministrativo, si completa con la previsione dell'ari *187-quinquies* TUF, illustrato di seguito.

2. CONSIDERAZIONI GENERALI

La disciplina della responsabilità dell'ente con riguardo alle nuove fattispecie di illecito è articolata su due piani:

l'art. *187-quinquies* del TUF prevede che la Consob possa applicare sanzioni amministrative pecuniarie da 100 mila a 15 milioni di euro ovvero da 100 mila a 25 milioni di euro, rispettivamente per gli illeciti di abuso di informazioni privilegiate e di manipolazione del mercato e che la sanzione può essere aumentata fino a dieci volte il profitto o il prodotto conseguito dall'ente a seguito della commissione dell'illecito, se il profitto o il prodotto siano di rilevante entità;

l'art. 25-sexies del decreto n. 231/2001 stabilisce che il giudice, in sede penale, possa applicare una sanzione pecuniaria da quattrocento a mille quote, incrementabile fino a dieci volte il profitto o il prodotto conseguito dall'ente a seguito della commissione del reato, se questi siano di rilevante entità. Non sono previste sanzioni interdittive a carico dell'ente.

Pertanto, se la fattispecie di illecito presupposto assume rilevanza penale, l'eventuale responsabilità dell'ente sarà accertata in sede giudiziaria; se invece si tratta di un illecito amministrativo - posto in essere comunque nell'interesse o a vantaggio dell'ente - l'accertamento e l'applicazione delle relative sanzioni spetterà alla Consob. Al riguardo, il TUF chiarisce i rapporti tra i procedimenti amministrativo e penale (Capo V, artt. 187-decies e ss.) e, con riferimento ai profili di accertamento delle responsabilità dei soggetti coinvolti, stabilisce che *"il procedimento amministrativo di accertamento e il procedimento di opposizione di cui all'art. 187-septies non possono essere sospesi per la pendenza del procedimento penale avente ad oggetto i medesimi fatti o fatti dal cui accertamento dipende la relativa definizione"*.

Pertanto, una stessa fattispecie/notizia di illecito potrebbe contestualmente essere oggetto di un procedimento penale dinanzi al giudice ordinario e di un procedimento amministrativo presso la Consob, con un conseguente accertamento della responsabilità dell'ente per la medesima fattispecie sia in sede giudiziaria che amministrativa.

3. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI⁷

In tema di controlli, si evidenzia l'importanza di controlli di tipo *ex post* completi, tempestivi e sistematici. Peraltro, tali controlli, se noti a dipendenti e soggetti apicali, potrebbero costituire un valido disincentivo anche in via *ex ante*, che consentirebbe di alleggerire i controlli preventivi ed evitare un eccessivo rallentamento dell'attività ordinaria sui mercati. Inoltre, è importante che i controlli relativi agli abusi di mercato vengano effettuati esaminando tutti i possibili interessi che l'ente associato ha sui titoli sui quali opera.

Si sottolinea, altresì, l'opportunità di attivare le seguenti misure preventive di carattere generale: i) introduzione nel Codice etico sia di norme e divieti volti a prevenire gli abusi di mercato e l'adozione di comportamenti che potrebbero dare adito a situazioni di conflitto di interessi, sia di richiami al rispetto delle procedure; ii) previsione di specifiche sanzioni disciplinari per la violazione delle procedure e degli obblighi connessi agli abusi di mercato; iii) diffusione di adeguate informazioni al riguardo a tutto il personale.

⁷ Nell'elencazione dei comportamenti rilevanti sono riprodotti alcuni degli esempi contenuti nella Comunicazione Consob n. DME/5078692 del 29 novembre 2005, che, a sua volta, si rifà al documento "Market Abuse Directive. Level 3 - First set of CESR guidance and information on the common operation of the directive" del Committee of European Securities Regulators (CESR). Non sono stati riportati quegli esempi, contenuti sempre nella Comunicazione, che descrivono comportamenti propri degli intermediari. Per l'approfondimento dei contenuti si rinvia alla citata Comunicazione.

Infatti, le indicazioni contenute nelle Linee Guida di Confindustria sono state elaborate in considerazione della natura e delle caratteristiche peculiari della componente associativa, tenendo conto delle specificità proprie dei diversi settori industriali rappresentati. Esse sono quindi essenzialmente indirizzate ai soggetti (imprese ed enti) che operano, a vario titolo, nel complesso campo della produzione di beni e/o prestazione di servizi. In questo ambito possono rientrare, seppure in via residuale, soggetti emittenti che svolgono funzioni o attività tipiche di intermediazione finanziaria, di investimento in partecipazioni, ecc. Resta ferma in questi casi l'esigenza di essere compliant rispetto ai codici di comportamento predisposti da associazioni di categoria di settore.

Nella parte della tabella relativa all'abuso di informazioni privilegiate è riportato un elenco di eventi/circostanze che possono costituire la fonte di informazioni privilegiate che riguardano direttamente il soggetto emittente. Gli eventi e le informazioni indicate, che hanno un valore puramente esemplificativo e non esaustivo, sono riprese dal documento del CESR del luglio 2007 ("Market Abuse Directive. Level 3 - Second Set of CESR Guidance and Information on the Common Operation of the Directive to the Market" - CESR/06-562b, section 1.15), al quale si rinvia per una disamina più completa della casistica. Le suddette informazioni, utili per definire il contenuto ed i limiti delle fattispecie di abuso di informazioni privilegiate nonché di manipolazione informativa, possono agevolare gli enti nella individuazione delle aree a rischio e nella predisposizione del relativo sistema dei controlli preventivi.

Modalità di realizzazione dell'illecito - Aree a rischio illecito	Controlli preventivi	
	Specifici	Comuni alle due fattispecie
<p>Abuso di informazioni privilegiate</p> <p>Un soggetto in posizione apicale o un sottoposto che rientri in una delle categorie di cui all'art. 184, co. 1 TUF utilizza informazioni di cui è entrato in possesso e compie una delle seguenti operazioni:</p> <ul style="list-style-type: none"> • acquisto, vendita o altre operazioni, direttamente o indirettamente, su strumenti finanziari emessi dalla società o da società del gruppo; • comunicazione delle informazioni ad altri soggetti al di fuori dell'ordinario esercizio dell'attività lavorativa; • raccomandazione ad altri o induzione di altri soggetti ad acquistare, vendere o compiere altre operazioni su strumenti finanziari emessi dalla società o da società del gruppo. <p>Le stesse operazioni rilevano laddove poste in essere da soggetti sempre in posizione di apicali o sottoposti, che non rientrano tra quelli di cui all'art. 184, co. 1 TUF, ma che comunque vengano in possesso di informazioni privilegiate in occasione della preparazione o esecuzione di attività delittuose (art. 184, co. 2, TUF).</p> <p>Con riferimento al solo illecito amministrativo, le stesse operazioni rilevano anche qualora commesse dai soggetti di cui all'art. 187-bis, co. 4 TUF.</p> <p>Risultano pertanto potenzialmente a rischio illecito le seguenti aree o funzioni:</p> <ul style="list-style-type: none"> • organi sociali; • area Finanza; 	<p>Introduzione/integrazione di principi, regolamenti e procedure (es. regolamenti <i>sull'internal dealing</i>) su utilizzo e diffusione delle informazioni privilegiate, anche coordinando gli interventi diretti a garantire la riservatezza delle informazioni privilegiate con le misure di sicurezza già previste e introdotte in attuazione del d.lgs. n. 196/2003. Sarebbe opportuno:</p> <ul style="list-style-type: none"> • prevedere uno specifico obbligo del titolare (o del responsabile del trattamento) di riporto periodico diretto al vertice operativo aziendale in ordine alla politica adottata dall'impresa in materia di gestione e protezione dei flussi informativi; • predisporre i Registri delle persone che hanno accesso alle informazioni privilegiate; • assicurare la riservatezza delle informazioni mediante l'adozione di misure di confidenzialità volte a garantire la sicurezza 	<p>Previsione di un sistema definito di responsabilità del vertice aziendale e di connesse deleghe coerenti.</p> <p>Programma di informazione/formazione periodica di amministratori, <i>management</i> e dipendenti delle aree/funzioni aziendali a rischio, nonché delle persone inserite nei Registri delle persone che hanno accesso alle informazioni privilegiate, su normativa in materia di abusi di mercato e relative procedure interne.</p> <p>Individuazione di soggetti rilevanti, procedure autorizzative e operazioni da essi effettuate, anche per interposta persona, aventi ad</p>

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 64 di 85
------------------------------	---------------------	-----------------	--------------------

<ul style="list-style-type: none"> • area Tesoreria; • area Legale, societario • area Comunicazione, ufficio stampa; • <i>investor relations</i>; • altri soggetti inseriti nei registri delle persone che hanno accesso alle informazioni privilegiate. 	<p>organizzativa, fisica e logica delle informazioni privilegiate;</p> <ul style="list-style-type: none"> • specificare le modalità di condotta da adottare nei rapporti formali e informali con gli operatori della comunità finanziaria, con i media e con i terzi in genere. 	<p>oggetto azioni e strumenti finanziari;</p> <p>Procedure autorizzative e di controllo per comunicati stampa, informativa societaria, diffusione delle informazioni privilegiate al mercato ecc. e procedure per la comunicazione delle società controllate alla società controllante di informazioni richieste ai fini degli adempimenti di gestione, comunicazione e diffusione delle informazioni privilegiate;</p> <p>Comunicazione sistematica all'OdV da parte di amministratori, <i>management</i> e dipendenti delle aree/funzioni aziendali a rischio, di fatti e/o comportamenti sintomatici</p>
Manipolazione di mercato⁸		
<p>Operazioni false o fuorvianti (art. 187-ter, co. 3, lett. a), TUF):</p> <ul style="list-style-type: none"> • Operazioni fittizie (<i>wash trades</i>) • Alterazione del quadro delle operazioni (<i>painting the tape</i>) • Ordini abbinati in modo improprio • <p>Inserimenti di ordini nel mercato senza l'intenzione di eseguirli Risultano pertanto potenzialmente a rischio illecito le seguenti aree: i) Finanza; ii) Tesoreria.</p> <p>Operazioni che fissano i prezzi a livelli anomali o artificiali (art.</p>	<p>Introduzione/integrazione di principi, regolamenti e procedure in tema di abusi di mercato, anche mediante riferimento alla casistica riportata dalla Consob nella citata Comunicazione del novembre 2005.</p>	

⁸ Nell'ambito delle condotte manipolative riportate nella tabella che segue, in via esemplificativa, si segnala che le società emittenti o in via di quotazione, i soggetti che le controllano (e, più in generale, le società in rapporto di controllo con società quotate o in via di quotazione) ovvero coloro che detengono in esse una partecipazione rilevante (c.d. *large investors*) dovranno prestare particolare attenzione alle seguenti fattispecie: i) "costituzione di una soglia minima al corso dei prezzi"; ii) "celare la proprietà"; iii) "comprimere in modo abusivo il mercato".

Per quanto riguarda gli investitori molto attivi sui mercati, le operazioni manipolative più caratteristiche sono quelle di: i) "*trading on one market to improperly position the price of a financial instrument on a related market*"; iii) "*pump and dump*"; iii) "*trash and cash*".

187-ter, co. 3, lett. b), TUF):

- Segnare il prezzo in chiusura (*marking the close*)
- Colludere sul mercato secondario dopo un collocamento effettuato nell'ambito di un'offerta al pubblico
- Comprimere in modo abusivo il mercato (*abusive squeeze*)
- Costituzione di una soglia minima al corso dei prezzi
- Operazioni effettuate in un mercato per influenzare impropriamente i prezzi di uno strumento finanziario in un mercato correlato

Risultano pertanto potenzialmente a rischio illecito le seguenti aree: i) Finanza; ii) Tesoreria.

Operazioni che utilizzano artifici, inganni o espedienti (187-ter, co. 3, lett. c), TUF):

- Celare la proprietà (*concealing ownership*)
- Diffusione di informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo
- Gonfiare e scaricare (*Pump and dump*)
- Screditare e incassare (*Trash and cash*)
- Aprire una posizione e chiuderla immediatamente dopo che è stata resa nota al pubblico (*opening a position and closing it immediately after its public disclosure*)

Risultano pertanto potenzialmente a rischio reato le seguenti aree/funzioni: i) Componenti organi sociali; ii) Finanza; iii) Tesoreria; iv) Legale, societario; v) Comunicazione, Ufficio stampa; vi) *Investor*

Per le sole società emittenti che non svolgano direttamente attività di intermediazione, previsione della possibilità di avvalersi, per l'esecuzione di operazioni su strumenti finanziari, di intermediari abilitati che attestino di avere adottato adeguate procedure informatiche.

di operazioni di *market abuse* e conseguente obbligo dell'OdV di riferire tempestivamente all'organo dirigente e/o di controllo le situazioni che possono integrare un illecito, ai fini delle iniziative e dei provvedimenti di rispettiva competenza.

relations.

Diffusione di informazioni false o fuorvianti (187-ter, co. 1, TUF):

Questo tipo di manipolazione del mercato implica la diffusione di informazioni false o fuorvianti senza richiedere necessariamente la presenza di operazioni sul mercato. Inoltre, comprende i casi in cui la creazione dell'indicazione fuorviante deriva da un mancato rispetto della disciplina in materia di comunicazione di informazioni rilevanti, soggette a obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati (oltre alle ipotesi di diffusione spontanea delle informazioni false o fuorvianti). Ad esempio, quando un emittente omette di diffondere adeguatamente un'informazione privilegiata, come definita dall'articolo 114, co. 1, e il risultato è che il pubblico venga plausibilmente fuorviato. In ogni caso, il mancato rispetto degli obblighi di comunicazione rileva solo qualora risulti di particolare gravità (un chiaro indice di gravità è, ad esempio, la sussistenza della volontà di fuorviare il pubblico).

Fattispecie:

- Diffusione di informazioni false o fuorvianti tramite mezzi di comunicazione
- Altri comportamenti preordinati alla diffusione di informazioni false o fuorvianti

Risultano pertanto potenzialmente a rischio illecito le seguenti aree/funzioni: i) Componenti organi sociali; ii) Finanza; iii) Tesoreria; iv) Legale, societario; v) Comunicazione, Ufficio stampa; vi) *Investor relations*; vii) Commerciale.

Reati presupposto

Reati presupposto		
Codice penale	art. 589	Omicidio colposo
	art. 590	Lesioni personali colpose

1. CONSIDERAZIONI GENERALI

La legge 123/2007 ha per la prima volta previsto la responsabilità dell'ente in dipendenza di un reato colposo.

Tale circostanza impone un coordinamento con l'art. 5 del decreto 231, che definisce il criterio oggettivo di imputazione della responsabilità dell'ente, subordinandola all'esistenza di un *interesse o vantaggio* per l'ente⁹, nonché con l'esimente di cui all'art. 6, nella parte in cui richiede la prova della elusione fraudolenta del modello organizzativo, sicuramente incompatibile con una condotta colposa. A tal proposito, *l'impasse* si potrebbe superare facendo ricorso ad una interpretazione che, tenendo conto del diritto di difesa e del principio di uguaglianza, permetta di prescindere da tale prova o quantomeno di disancorare il concetto di "elusione fraudolenta" dalle tipiche fattispecie proprie del codice penale e di assumerlo in termini di intenzionalità della sola condotta dell'autore (e non anche dell'evento) in violazione delle procedure e delle disposizioni interne predisposte e puntualmente implementate dall'azienda per prevenire la commissione degli illeciti di cui si tratta o anche soltanto di condotte a tali effetti "pericolose".

Questa interpretazione si fonda sui seguenti presupposti. Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche. In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare la norme di prevenzione e protezione. Tale soggetto può quindi individuarsi, ai sensi del decreto 81/2008, nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori.

⁹ Sul punto cfr. *retro*, cap. I.

I delitti contemplati dagli artt. 589 e 590 c.p. sono caratterizzati dall'aggravante della negligente inosservanza delle norme antinfortunistiche. L'elemento soggettivo, dunque, consiste nella cd. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte a impedire gli eventi dannosi previsti dalla norma incriminatrice.

Il concetto di colpa specifica rimanda all'art. 43 c.p., nella parte in cui si prevede che il delitto è colposo quando l'evento, anche se preveduto ma in ogni caso non voluto dall'agente, si verifica a causa dell'inosservanza di norme di leggi, regolamenti, ordini o discipline.

L'individuazione degli obblighi di protezione dei lavoratori è tutt'altro che agevole, infatti oltre decreto 81/2008 e agli altri specifici atti normativi in materia, la giurisprudenza della Cassazione ha precisato che tra le norme antinfortunistiche di cui agli artt. 589, comma 2, e 590, comma 3, c.p., rientra anche l'art. 2087 c.c., che impone al datore di lavoro di adottare tutte quelle misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica dei lavoratori.

Tale norma non può però intendersi come prescrivente l'obbligo generale ed assoluto di rispettare ogni cautela possibile ed "innominata" ad evitare qualsivoglia danno, perché in tal modo significherebbe ritenere automatica la responsabilità del datore di lavoro ogni volta che il danno si sia verificato (Cass. civ., sez. lav., n. 3740/1995).

Prediligendo, inoltre, un approccio interpretativo sistematico che valuti il rapporto di interazione tra norma generale (art. 2087 c.c.) e singole specifiche norme di legislazione antinfortunistica previste dal decreto 81 del 2008, appare coerente concludere che:

- l'art. 2087 c.c. introduce l'obbligo generale contrattuale per il datore di lavoro di garantire la massima sicurezza tecnica, organizzativa e procedurale possibile;
- conseguentemente, l'elemento essenziale ed unificante delle varie e possibili forme di responsabilità del datore di lavoro, anche ai fini dell'applicabilità dell'art. 25-*septies* del decreto 231 del 2001, è uno solo ed è rappresentato dalla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili (come specificato dall'art. 3, comma 1, lett. b), del decreto 81/2008), alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche.

A specificare ulteriormente il generico dettato legislativo, può giovare la sentenza della Corte Costituzionale n. 312 del 18 luglio 1996 secondo cui l'obbligo generale di massima sicurezza possibile deve fare riferimento alle misure che nei diversi settori e nelle diverse lavorazioni, corrispondono ad applicazioni tecnologiche generalmente praticate e ad accorgimenti generalmente acquisiti, sicché penalmente censurata è solo la deviazione del datore di lavoro dagli standard di sicurezza propri, in concreto ed al momento, delle singole diverse attività produttive.

Il novero degli obblighi in materia antinfortunistica si accresce ulteriormente ove si consideri che secondo la migliore dottrina e la più recente giurisprudenza l'obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza nei termini sopra esposti (forme di protezione oggettiva), ma deve al contrario intendersi anche in maniera dinamica implicando l'obbligo di informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

Confindustria

Il datore di lavoro che abbia, secondo i criteri sopra esposti, adempiuto agli obblighi in materia di salute e sicurezza sul luogo di lavoro (sia generali ex art. 2087 c.c. che speciali ex decreto 81 del 2008), è responsabile del solo evento di danno che si sia verificato in occasione dell'attività di lavoro e abbia un nesso di derivazione effettiva con lo svolgimento dell'attività lavorativa.

La giurisprudenza prevede infatti una interruzione del nesso di causalità tra la condotta dell'agente e l'evento lesivo ogni qualvolta la condotta del lavoratore sia da considerare abnorme, ossia strana e imprevedibile e perciò stesso si ponga al di fuori di ogni possibilità di controllo da parte delle persone preposte all'applicazione delle misure di prevenzione contro gli infortuni sul lavoro. Conseguentemente deve ritenersi che rimangano fuori dall'ambito di rilevanza normativa (ai fini della responsabilità civile e penale) gli infortuni derivanti dalla sussistenza del cd. rischio elettivo ossia il rischio diverso da quello a cui il lavoratore sarebbe ordinariamente esposto per esigenze lavorative ed abnorme ed esorbitante rispetto al procedimento di lavoro e che il lavoratore affronta per libera scelta con atto volontario puramente arbitrario per soddisfare esigenze meramente personali.

Il quadro sopra esposto, sia pure in termini di estrema sintesi, riferito alla complessità dei presupposti formali e sostanziali della responsabilità del datore di lavoro per violazione di norme antinfortunistiche, consente di concludere che di fatto, con l'entrata in vigore della legge 123 del 2007, ogni azienda che registri una consistente frequenza di infortuni gravi, dovrebbe considerare inaccettabile il "rischio" di incorrere, oltre che nelle responsabilità di matrice civile e penale tipiche della materia, anche nelle ulteriori sanzioni del decreto 231 del 2001 per il fatto di non aver predisposto ed efficacemente attuato un idoneo Modello di Organizzazione, Gestione e Controllo.

Quest'ultimo, per essere efficacemente attuato, potrà utilmente essere integrato con il "sistema" degli adempimenti aziendali nascenti dagli obblighi di prevenzione e protezione imposti dall'ordinamento legislativo (v. sopra) e, qualora presenti, con le procedure interne nascenti dalle esigenze di gestione della sicurezza sul lavoro.

Da qui l'opportunità che l'azienda ponga in essere azioni mirate volte garantire la suddetta integrazione (anche in vista della successiva eventuale verifica da parte del Giudice) ed in particolare:

- effettuazione di una mappatura del rischio approfondita e orientata secondo le specificità dell'attività produttiva presa in considerazione;
- attenta verifica ed eventuale integrazione delle procedure interne di prevenzione ai sensi del decreto 231 in coerenza con la specificità dei rischi di violazione delle norme richiamate dall'art. 25-*septies*; a tal fine sarà importante tenere conto e armonizzare tutte le attività già svolte, anche in materia di gestione della sicurezza, evitando inutili quanto costose duplicazioni;
- valutazione ed individuazione dei raccordi tra i vari soggetti coinvolti nel sistema di controllo ai sensi del decreto 231 e delle normative speciali in materia di sicurezza e salute sui luoghi di lavoro, con particolare riferimento alla previsione di un sistema integrato di controllo riguardante il Responsabile dei servizi di prevenzione e protezione (RSPP o altro soggetto giuridicamente equivalente) qualificabile come controllo tecnico-operativo o di primo grado, e l'Organismo di Vigilanza.

Art. 25-octies d.lgs. 231/2001 - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Reati presupposto		
Codice penale	art. 648	Ricettazione
	art. 648-bis	Riciclaggio
	art. 648-ter	Impiego di denaro, beni o utilità di provenienza illecita

1. CONSIDERAZIONI GENERALI

Con il decreto 231 del 21 novembre 2007 il legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio), e alla direttiva 2006/70/CE della Commissione che ne reca misure di esecuzione.

L'intervento normativo comporta un riordino della complessa normativa antiriciclaggio presente nel nostro ordinamento giuridico, tra l'altro estendendo la responsabilità amministrativa degli enti ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza. Inoltre, abroga i commi 5 e 6 dell'art. 10 della l. n. 146/2006, di contrasto al crimine organizzato transnazionale, che già prevedevano a carico dell'ente la responsabilità e le sanzioni ex 231 per i reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648-bis e 648-terc.p.), se caratterizzati dagli elementi della transnazionalità, secondo la definizione contenuta nell'art. 3 della stessa legge 146/2006. Ne consegue che ai sensi dell'art. 25-octies, decreto 231/2001, l'ente sarà ora punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un *interesse o vantaggio* per l'ente medesimo.

La finalità del decreto 231/2007, come successivamente modificato, consiste nella protezione del sistema finanziario dal suo utilizzo a fini di riciclaggio o di finanziamento del terrorismo. Tale tutela viene attuata con la tecnica della prevenzione per mezzo di apposite misure e obblighi di comportamento che, ad eccezione dei limiti all'uso del contante e dei titoli al portatore (art. 49) che sono applicabili alla generalità dei soggetti, riguardano una vasta platea di soggetti individuati agli artt. 10, comma 2, 11, 12, 13 e 14 del decreto: banche, intermediari finanziari, professionisti, revisori contabili e operatori che svolgono attività il cui esercizio è subordinato a licenze, autorizzazioni, iscrizioni in albi/registri o dichiarazioni di inizio attività richieste da norme di legge (es. recupero crediti per conto terzi, custodia e trasporto di denaro contante, di titoli o valori con o senza l'impiego di guardie giurate, agenzie di affari in mediazione immobiliare, case da gioco, commercio di oro per finalità industriali o di investimento, fabbricazione, mediazione e commercio di oggetti preziosi, fabbricazione di oggetti preziosi da parte di imprese artigiane,

commercio di cose antiche, esercizio di case d'asta o galleria d'arte, ecc.). Nei loro confronti trovano applicazione gli obblighi di cui al citato decreto 231/2007, in tema di adeguata verifica della clientela, tracciabilità delle operazioni, adeguata formazione del personale e segnalazione di operazioni sospette (cfr. artt. 41 e ss. decreto 231/2007), nel rispetto di limiti, modalità e casi specificamente indicati dallo stesso decreto e precisati, da ultimo, nei provvedimenti di Banca d'Italia del 3 aprile 2013, nonché le specifiche disposizioni e istruzioni applicative, in materia di identificazione/registrazione/conservazione delle informazioni/segnalazione delle operazioni sospette, dettate a carico degli operatori c.d. "non finanziari" dal decreto del MEF n. 143 del 3 febbraio 2006 e dal provvedimento UIC del 24 febbraio 2006, cui si rinvia per approfondimenti. Si evidenzia che questi ultimi provvedimenti devono essere interpretati alla luce dei chiarimenti forniti dal Ministero dell'Economia e delle Finanze con la nota del 19 dicembre 2007, che individua le disposizioni di normativa secondaria da considerare ancora compatibili a seguito dell'entrata in vigore del d.lgs. n. 231/2007.

L'inadempimento a siffatti obblighi viene sanzionato dal decreto con la previsione di illeciti amministrativi e di reati penali cd. "reati-ostacolo", tendenti a impedire che la progressione criminosa giunga alla realizzazione delle condotte integranti ricettazione, riciclaggio o impiego di capitali illeciti.

A tal proposito, merita di essere considerato l'articolo 52 del decreto che obbliga i diversi organi di controllo di gestione - nell'ambito dell'ente destinatario della normativa -, tra cui l'Organismo di vigilanza, a vigilare sull'osservanza della normativa antiriciclaggio e a comunicare le violazioni delle relative disposizioni di cui vengano a conoscenza *nell'esercizio dei propri compiti* o di cui abbiano altrimenti notizia. Tali obblighi di comunicazione riguardano in particolar modo le possibili infrazioni relative alle operazioni di registrazione, segnalazione e ai limiti all'uso di strumenti di pagamento e di deposito (contante, titoli al portatore, conti e libretti di risparmio anonimi o con intestazioni fittizie) e sono destinati ad avere effetto sia verso l'interno dell'ente (titolare dell'attività o legale rappresentante) che verso l'esterno (autorità di vigilanza di settore, Ministero Economia e Finanze).

La lettera della norma potrebbe far ritenere sussistente in capo a tutti i suddetti organi una posizione di garanzia ex art. 40, comma 2, c.p. finalizzata all'impedimento dei reati di cui agli artt. 648, 648-bis e 648-ter c.p.

Una corretta e coerente interpretazione dovrebbe invece tenere in debito conto i differenti poteri/doveri assegnati ai diversi organi di controllo, sia dalla normativa in questione che dalle disposizioni generali dell'ordinamento (*in primis*, il codice civile). Mentre per alcuni dei suddetti organi di controllo sembrerebbe sussistere una tale posizione di garanzia, con specifico riferimento all'Organismo di vigilanza una simile responsabilità appare del tutto incompatibile con la natura dei poteri/doveri ad esso originariamente attribuiti dalla legge.

Pertanto, dovrebbe prevalere un'interpretazione sistematica della norma che limiti il dovere di vigilanza di cui al comma 1 dell'articolo 52 e le relative responsabilità all'adempimento degli obblighi informativi previsti dal comma 2 della medesima disposizione. In altri termini, l'adempimento dei doveri di informazione a fini di antiriciclaggio deve essere commisurato ai concreti poteri di vigilanza spettanti a ciascuno degli organi di controllo contemplati dal comma 1 dell'articolo 52, nell'ambito dell'ente di appartenenza che sia destinatario della normativa.

Ne deriva che il dovere di informativa dell'Organismo di vigilanza non può che essere parametrato alla funzione, prevista dall'art. 6, comma 1, lett. b) del decreto 231, di vigilare sul funzionamento e sull'osservanza dei modelli e, con specifico riferimento all'antiriciclaggio, di comunicare quelle violazioni di cui venga a conoscenza nell'esercizio delle proprie funzioni o nelle ipotesi in cui ne abbia comunque notizia (es. su segnalazione di dipendenti o altri organi dell'ente). Tale ultima previsione risulta, d'altra parte, coerente con gli obblighi di informazione stabiliti dalla legge nei confronti dell'Organismo medesimo allo scopo di migliorare l'attività di pianificazione dei controlli e di vigilanza sul modello da parte di quest'ultimo.

Tale chiave di lettura, senza riconoscere una posizione di garanzia, in assenza di effettivi poteri impeditivi dell'Organismo di vigilanza rispetto alle fattispecie di reato in esame, viene completata dalla sanzione penale della reclusione fino a 1 anno e della multa da 100 a 1000 euro in caso di mancato adempimento dei suddetti obblighi informativi (art. 55, comma 5).

Vale la pena sottolineare che quello in esame è l'unico caso in cui il legislatore abbia espressamente disciplinato una specifica fattispecie di reato a carico dell' Organismo di vigilanza (reato omissivo proprio), peraltro a seguito del riconoscimento di una *atipica* attività a rilevanza esterna dello stesso.

La responsabilità amministrativa dell'ente per i reati previsti dagli art. 648, 648-bis e 648-ter, c.p. è limitata alle ipotesi in cui il reato sia commesso nell'interesse o a vantaggio dell'ente medesimo.

Considerato che le fattispecie delittuose in questione possono essere realizzate da chiunque, trattandosi di reati comuni, si dovrebbe ritenere che la ricorrenza del requisito oggettivo dell'interesse o vantaggio vada esclusa ogni qual volta non vi sia attinenza tra la condotta incriminata e l'attività d'impresa esercitata dall'ente.

Tale attinenza, ad esempio, potrebbe ravvisarsi nell'ipotesi di acquisto di beni produttivi provenienti da un delitto di furto, ovvero nel caso di utilizzazione di capitali illeciti per l'aggiudicazione di un appalto, ecc. Viceversa, non è ravvisabile l'interesse o il vantaggio per l'ente nell'ipotesi in cui l'apicale o il dipendente acquistino beni che non abbiano alcun legame con l'esercizio dell'impresa in cui operano. Lo stesso può dirsi per l'impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale.

Peraltro, anche nel caso in cui l'oggetto materiale della condotta di ricettazione o di riciclaggio, ovvero l'attività economica o finanziaria nel caso del reato ex art. 648-ter c.p., siano pertinenti rispetto alla specifica attività d'impresa, occorre pur sempre un accertamento in concreto da parte del giudice, da condurre caso per caso, circa la sussistenza dell'interesse o del vantaggio per l'ente.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Le attività aziendali da prendere in considerazione ai fini della prevenzione di tali reati possono essere suddivise in due macrocategorie:

1. attività con soggetti terzi, relative ai rapporti instaurati tra società e soggetti terzi;
2. attività infragruppo, poste in essere nell'ambito dei rapporti intercorrenti fra società appartenenti allo stesso gruppo.

Aree e attività aziendali a rischio	Controlli preventivi
<p>Aree aziendali a rischio:</p> <ul style="list-style-type: none"> • Amministrazione (in particolare, Tesoreria, Personale, Ufficio contratti/gare, ecc.) • Commerciale • Finanza • Direzione acquisiti; • Marketing¹⁰. <p>Attività aziendali a rischio in relazione a:</p> <ul style="list-style-type: none"> • rapporti con soggetti terzi: contratti di acquisto e/o di vendita con controparti; transazioni finanziarie con controparti; investimenti con controparti; sponsorizzazioni. • rapporti infragruppo: 	<p>Verifica dell'attendibilità commerciale e professionale dei fornitori e <i>partner</i> commerciali/finanziari, sulla base di alcuni indicatori di anomalia previsti dall'art. 41, comma 2 del d. lgs. n. 231/2007 e individuati con successivi provvedimenti attuativi (es. dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di "persone politicamente esposte", come definite all'art. 1 dell'Allegato tecnico del D.lgs. 21 novembre 2007, n. 231, di attuazione della direttiva 2005/60/CE)¹¹.</p> <p>Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni.</p> <p>Controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie¹².</p> <p>Verifiche sulla Tesoreria (rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.).</p> <p>Determinazione dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard.</p> <p>Identificazione di una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard.</p> <p>Identificazione di un organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e</p>

¹⁰ La direzione acquisti e il *marketing* si reputano esposti sia al rischio riciclaggio che al rischio di finanziamento del terrorismo (compreso anch'esso tra i reati-presupposto del decreto 231, all'art. 25-*quater*, co. 4). In particolare, la direzione acquisti è responsabile dei rapporti con terzi fornitori, che potenzialmente possono risultare coinvolti in episodi di riciclaggio o di ricettazione (art. 648 c.p. - ad es. possesso di merce rubata). La direzione *Marketing* spesso è coinvolta nella sponsorizzazione di ONLUS/ONG (soggetti a rischio di finanziamento del terrorismo) o nel pagamento di prestazioni immateriali, servizi di consulenza (che possono a loro volta rilevare quali veicoli di riciclaggio di denaro).

¹¹ Gli indicatori di anomalia da tener presenti al fine di contrastare i fenomeni di riciclaggio o di finanziamento del terrorismo sono diversi dalle semplici anomalie contabili, riferendosi ad esempio alla sede del soggetto controparte, alle modalità e ai prezzi dell'offerta o del bene ed altri indici specifici individuati dalla normativa (persone politicamente esposte o altre categorie ritenute esposte).

¹² Le operazioni infragruppo, l'utilizzo di schermi societari e/o strutture fiduciarie sono indici di operazioni sospette a fini di antiriciclaggio, peraltro già utilizzati e evidenziati dalla magistratura in indagini su reati di natura finanziaria.

<p>contratti infragruppo di acquisto e/o di vendita;</p> <p>gestione dei flussi finanziari;</p> <p>investimenti infragruppo.</p>	<p>responsabilità.</p> <p>Specifica previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio.</p> <p>Determinazione dei criteri di selezione, stipulazione ed esecuzione di <i>accordi/joint-ventures</i> con altre imprese per la realizzazione di investimenti. Trasparenza e tracciabilità degli <i>accordi/joint-ventures</i> con altre imprese per la realizzazione di investimenti.</p> <p>Verifica della congruità economica di eventuali investimenti effettuati in <i>joint ventures</i> (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di due <i>diligence</i>).</p> <p>Verifica sul livello di adeguamento delle società controllate rispetto alla predisposizione di misure e controlli antiriciclaggio.</p> <p>Applicazione dei controlli preventivi specifici (protocolli) previsti anche in riferimento ai reati nei rapporti con la Pubblica Amministrazione, ai reati societari e ai reati di <i>market abuse</i>;</p> <p>Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.</p>
--	---

Art. 25-novies d.lgs. 231/2001 - Delitti in materia di violazione del diritto d'autore

Reati presupposto		
L. 633/1941	art. 171	Divulgazione di opere dell'ingegno attraverso rete telematica
	art. 171-bis	Reati in materia di <i>software</i> e banche dati
	art. 171-ter	Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche
	art. 171 - <i>septies</i>	Violazioni nei confronti della SIAE
	art. 171 - <i>octies</i>	Manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato

1. CONSIDERAZIONI GENERALI

I reati presupposto inseriti nell'art. 25-novies non sono fattispecie di reato di esclusivo interesse delle imprese operanti nello specifico settore software/audiovisivo, ma, al contrario, alcune fattispecie di reato impongono, alla quasi totalità dei soggetti collettivi portatori di interesse economico che intendono contenere i rischi, l'esigenza di porre in essere specifiche misure e protocolli.

Tali reati potrebbero essere compiuti nel perseguimento degli interessi della società, a prescindere dall'eventuale impiego - a tal fine - di beni aziendali (come gli strumenti informatici, i sistemi di diffusione di informazioni e le attrezzature per la duplicazione di testi).

Al fine di prevenire reati ipotizzabili anche senza l'utilizzo di beni aziendali, si consiglia di:

- formulare inviti generali al rispetto delle norme in materia di proprietà intellettuale;
- elaborare clausole riferite all'osservanza anche da parte dei terzi contraenti delle norme in materia di proprietà intellettuale;
- vietare l'impiego per finalità aziendali di beni tutelati da diritti acquisiti in elusione dei relativi obblighi o comunque con modalità difformi da quelle previste dal titolare;
- prevedere principi etici dedicati.

Al fine di prevenire reati ipotizzabili con l'utilizzo di beni aziendali, oltre ai controlli di cui sopra, si consiglia di:

- vietare l'impiego di beni aziendali (come fotocopiatrici, sito web, copisterie o altro) al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito;
- controllare i mezzi di comunicazione interni ed esterni alla società (es. sito web, radio ufficiale, stampa, e altri canali ancora), in grado di diffondere opere protette.

Infine, nel caso particolare in cui gli illeciti contro la proprietà intellettuale si realizzino con l'impiego di sistemi informatici aziendali, possono rivelarsi utili anche le misure auspicabili anche per la prevenzione dei reati informatici richiamati dagli artt. 24, 24-bis e 25-quinquies del decreto 231, quali ad esempio lo sviluppo, la gestione e il monitoraggio delle infrastrutture informatiche o la presenza del cd. supervisore informatico.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Fattispecie incriminatrici - Modalità di realizzazione del reato	Controlli preventivi
<p>Art. 171, comma 1, lettera a), l. 633/1941 <i>File sharing</i>: condivisione o scambio di file in violazione della normativa del diritto d'autore e, comunque, al di fuori degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale. <i>Upload/download</i>: immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche.</p> <p>Art. 171, comma 3, l. 633/1941 Riproduzione, messa a disposizione, diffusione, vendita, rappresentazione di un'opera altrui non destinata alla pubblicazione.</p>	<p>Invito a rispettare le norme in materia di proprietà intellettuale.</p> <p>Controllo dei mezzi di comunicazione aziendali.</p> <p>Controllo dei sistemi informatici (filtro dei siti in conferenti, regole <i>firewall</i>, controllo dei livelli di traffico, controllo dei procedimenti di <i>file sharing</i>).</p> <p>Divieto di impiegare beni aziendali per adottare condotte che violino la tutela dei diritti d'autore.</p> <p>Clausole riferite all'osservanza delle norme in materia di proprietà intellettuale nei rapporti con i terzi contraenti.</p>
<p>Art. 171 -bis, l. 633/1941 <i>Undelicensing</i>: violazioni delle condizioni di licenza di un <i>software</i>. <i>Hard disk loading</i>: vendita e relativo acquisto per l'azienda di computer sui quali sono installati <i>software</i> piratati. Utilizzazione non autorizzata di banche dati.</p>	
<p>Art. 171-ter, l. 633/1941</p>	

Duplicazione, riproduzione, trasmissione o diffusione abusiva in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio.

Art. 171 -septies, l. 633/1941

Violazioni verso la SIAE.

Art. 171 -octies, l. 633/1941

Distribuzione e installazione di dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone.

Art. 25-decies d.lgs. 231/2001 - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

La Legge 3 agosto 2009, n. 116 (recante *"Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale."*) ha introdotto il reato presupposto di induzione a non rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis, c.p.), inserendo l'art. 25-decies nel decreto 231.

L'art. 377-bis c.p. sanziona le condotte poste in essere da chiunque, facendo ricorso ai mezzi della violenza, della minaccia o della "offerta o promessa di denaro o di altra utilità", induca a non rendere dichiarazioni, ovvero a renderle mendaci, tutti coloro che sono chiamati a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, nel caso in cui abbiano facoltà di non rispondere. Le condotte induttive individuabili nella struttura del delitto di cui all'art. 377-bis c.p. devono realizzarsi attraverso mezzi tassativamente delineati dalla norma incriminatrice e dunque consistere in una violenza, una minaccia, ovvero un'offerta o promessa di denaro o di altra utilità.

La scelta di reprimere penalmente condotte illecite finalizzate, in via diretta o indiretta, a inquinare il corretto svolgimento del contraddittorio e la genuinità dei suoi risultati probatori risulta volta ad adeguare la disciplina interna sui delitti contro l'amministrazione della giustizia alle fondamentali indicazioni di principio espresse a livello internazionale, come previsto dall'art. 24 della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale.

Con riferimento ai presidi di rischio che possono essere adottati dall'ente, si rinvia alle indicazioni sopra fornite in sede di esame dell'art. 24-ter (cfr. pagg. 15 e seguenti).

Art. 25-undecies d.lgs. 231/2001 - Reati ambientali

Reati presupposto		
Codice penale	art. 727 bis	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette
	art. 733 bis	Distruzione o deterioramento di habitat all'interno di un sito protetto
Codice dell'Ambiente (D.lgs. 152/2006)	art. 137	Sanzioni penali in materia di scarichi di acque reflue
	art. 256	Reati in materia di gestione non autorizzata di rifiuti
	art. 257	Reati in materia di bonifica dei siti
	art. 258	Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
	art. 259	Traffico illecito di rifiuti
	art. 260	Attività organizzate per il traffico illecito di rifiuti
	art. 260 bis	Sistema informatico di controllo della tracciabilità dei rifiuti
	art. 279	Reati in materia di tutela dell'aria e di riduzione delle emissioni in atmosfera
L. 150/1992	art. 1 - 3 bis, 6	Reati in materia di tutela di specie animali e vegetali in via di estinzione
L. 549/1993	art. 3	Reati in materia di ozono e atmosfera
D.lgs. 202/2007	art. 8, 9	Inquinamento doloso e colposo provocato dalle navi

1. CONSIDERAZIONI GENERALI

La responsabilità dell'ente è stata estesa ai reati ambientali dal d.lgs. 121/2011, emanato in attuazione della direttiva 2008/99/CE.

L'Unione Europea ha mostrato preoccupazione per la diffusione degli illeciti in materia ambientale, i cui effetti spesso si propagano anche oltre le frontiere degli Stati in cui i reati vengono commessi. Ha dunque imposto agli Stati membri di perseguire penalmente condotte che "provocino o possano provocare" pregiudizi all'ambiente e siano tenute "intenzionalmente o per grave negligenza". Per le sole "gravi violazioni" della disciplina europea in materia ambientale, i legislatori nazionali sono stati vincolati a introdurre sanzioni efficaci, proporzionate e dissuasive sia per la persona fisica che per l'ente.

I punti cardine della disciplina europea sulla tutela penale dell'ambiente sono dunque tre:

- l'incriminazione di gravi violazioni, dannose o almeno concretamente pericolose per l'ambiente;
- la commissione dei reati con dolo o grave negligenza;
- la previsione di sanzioni caratterizzate da efficacia, proporzionalità e dissuasività.

La disciplina legislativa italiana rispecchia in parte l'impulso proveniente dall'Unione Europea.

Anzitutto, dei reati ambientali presupposto di responsabilità ai sensi del decreto 231 solo alcuni sono concepiti come reati di danno o di pericolo concreto; altri incriminano condotte espressive di un pericolo meramente astratto. Ne consegue che, in questi casi, non è imposto al giudice di verificare in concreto la sussistenza di un pericolo, il quale viene concepito come presupposto della mera condotta illecita. Non essendo richiesta la dimostrazione di un'effettiva pericolosità della condotta, non è ammessa alcuna prova contraria in ordine all'insussistenza del pericolo.

Una simile impostazione, però, potrebbe suscitare perplessità sia rispetto alla già evocata disciplina europea, sia rispetto al principio costituzionale di offensività. Quest'ultimo, infatti, tollera l'incriminazione di fatti la cui pericolosità risulti insita nella condotta e non esiga ulteriori verifiche concrete, ma con riferimento a beni giuridici intangibili, cui ben si attaglia l'incriminazione di condotte censurabili in sé con l'antigiuridicità sul piano economico-sociale (per esempio la detenzione e il porto illegale di armi). Il bene ambiente è caratterizzato da un substrato empirico che consente di apprezzare l'effettiva sussistenza di una lesione in termini di pericolo o di danno. Dunque il legislatore non potrebbe anticipare la soglia del penalmente rilevante fino a colpire ogni mera violazione di norme o atti amministrativi.

Diversi reati ambientali, poi, colpiscono violazioni meramente formali. Si pensi, per esempio, a talune incriminazioni contenute nel Codice dell'ambiente: scarico di acque reflue industriali senza o in violazione di autorizzazione oppure superando i limiti tabellari fissati dal legislatore (art. 137); gestione non autorizzata di rifiuti (art. 256, comma 1, lett. a), comma 3, primo periodo, comma 5); violazione degli obblighi di comunicazione relativi al trasporto di rifiuti (art. 258); traffico illecito di rifiuti (art. 259) o superamento dei valori limite di emissione in atmosfera di sostanze inquinanti (art. 279).

La maggior parte dei reati richiamati è sanzionabile anche a titolo di colpa. Si tratta quasi sempre di contravvenzioni, come si desume dal tipo di sanzioni irrogabili: arresto e ammenda, in luogo di reclusione e multa, espressive della natura delittuosa del reato, ai sensi dell'articolo 17 del codice penale.

Sul piano della disciplina, dalla qualificazione contravvenzionale discende l'indifferenza, sul piano dell'elemento soggettivo del reato, tra dolo e colpa. La punibilità delle contravvenzioni per colpa, dunque, non esige l'esistenza di una previsione espressa, a differenza di quanto accade per i delitti, ma è sufficiente che la condotta sia cosciente e volontaria (art. 42, ultimo comma, c.p.).

In base a questa disciplina, dunque, gli illeciti ambientali in prevalenza sono punibili indipendentemente dal grado di colpa con cui sono commessi, anche se l'agente ha agito per semplice imprudenza o imperizia. Anche in questa prospettiva sembra profilarsi lo scostamento dalle indicazioni dell'Unione Europea, che vincolano l'incriminazione alla "grave negligenza".

Una simile estensione dell'area del penalmente rilevante si riflette in punto di responsabilità da reato degli enti. I modelli organizzativi, infatti, per aspirare al riconoscimento di efficacia esimente, qualora si verificano reati ambientali, devono contemplare misure idonee a evitare la commissione di un illecito anche solo per negligenza o imprudenza.

Infine, si segnala che il Decreto Legge n. 136/2013 ha introdotto nel Codice dell'ambiente il nuovo delitto di combustione illecita di rifiuti (art. 256-*bis*), che sanziona la persona fisica titolare dell'impresa o il responsabile dell'attività comunque organizzata, anche per l'omessa vigilanza sull'operato degli autori del delitto riconducibili all'impresa. In tal caso, ai titolari d'impresa o responsabili dell'attività sono applicabili le sanzioni interdittive di cui all'art. 9, co. 2 del decreto 231, mentre non è prevista la responsabilità dell'ente.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Fattispecie incriminatrici - Aree a rischio reato	Controlli preventivi
<p>Art. 727, 733 <i>bis</i> c.p.; art. 137, 279 cod. ambiente</p> <p>Gestione degli scarichi idrici Gestione delle emissioni atmosferiche</p> <p>Costruzione, gestione e manutenzione di infrastrutture in relazione a possibili impatti sulle biodiversità</p>	<p>Identificazione e valutazione di:</p> <ul style="list-style-type: none"> • aspetti ambientali in funzione dei beni prodotti, dei servizi resi e delle attività svolte in condizioni operative normali, anomale, in condizioni di avviamento e di fermata e in situazioni di emergenza e di incidenti; • significatività in relazione agli impatti ambientali diretti e indiretti correlati, anche sulla base del contesto territoriale di riferimento, nel rispetto della normativa vigente e dei relativi provvedimenti autorizzativi; • misure di prevenzione, protezione e mitigazione degli impatti ambientali conseguenti alla valutazione di significatività degli aspetti ambientali. <p>Disciplina delle attività di ottenimento, modifica e rinnovo delle autorizzazioni ambientali, affinché siano svolte in osservanza delle prescrizioni normative vigenti. Dovrebbero prevedersi modalità di monitoraggio della necessità di richiesta di una nuova autorizzazione o di modifica/rinnovo di autorizzazioni preesistenti.</p>

	<p>Misura e monitoraggio delle prestazioni ambientali, definendo ruoli, responsabilità, modalità e criteri per l'esecuzione delle attività di:</p> <ul style="list-style-type: none"> • identificazione e aggiornamento dei punti di scarico/emissione e dei punti di campionamento; • definizione dei programmi dei campionamenti e delle analisi degli scarichi/emissioni in linea con quanto previsto dalle prescrizioni autorizzative e dalla normativa vigente; • monitoraggio dei dati riguardanti gli scarichi/emissioni, ivi compresi i certificati analitici e i campionamenti effettuati. <p>Trattamento dei superamenti dei valori limite autorizzati e azioni correttive, al fine di realizzare:</p> <ul style="list-style-type: none"> • investigazione interna dei superamenti rilevati dalle determinazioni analitiche effettuate su scarichi/emissioni; • risoluzione dei superamenti rilevati dalle determinazioni analitiche effettuate su scarichi o emissioni.
<p>Art. 727 bis, 733 bis c.p.; art. 257 cod. ambiente Tutte le attività che si inseriscono nel ciclo di vita di un impianto in relazione al quale insistano obblighi in materia ambientale, cioè:</p> <ul style="list-style-type: none"> • acquisizione; • esercizio; • dismissione. 	<p>Disciplina delle attività di manutenzione e ispezione degli impianti lungo tutto il loro ciclo di vita, definendo:</p> <ul style="list-style-type: none"> • ruoli, responsabilità e modalità di gestione degli impianti; • periodiche verifiche di adeguatezza, integrità e regolarità degli impianti • pianificazione, compimento e verifica delle attività di ispezione e manutenzione mediante personale esperto e qualificato. <p>Adozione e attuazione di uno strumento organizzativo che:</p> <ul style="list-style-type: none"> • regoli la scelta e lo svolgimento dei rapporti con fornitori o appaltatori, imponendo di tenere conto dei requisiti morali e tecnico-professionali degli appaltatori, comprese le necessarie autorizzazioni previste dalla normativa; • imponga di verificare la corrispondenza di quanto eventualmente fornito con le specifiche di acquisto e le migliori tecnologie disponibili in tema di tutela dell'ambiente, della salute e della sicurezza; • definisca modalità di inserimento di clausole contrattuali relative al rispetto della normativa ambientale rilevante nell'esecuzione del singolo contratto di fornitura o appalto.

GB Gnudi Bruno S.p.A.	MOG parte II	REV. 10/2017	PAGINA 82 di 85
<p>Gestione degli adempimenti e delle attività connessi alla bonifica, a seguito di un evento che sia potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali o le acque sotterranee.</p>	<p>Occorre adottare e attuare uno strumento normativo e organizzativo che definisca ruoli, responsabilità, modalità e criteri per la gestione delle attività finalizzate alla bonifica dei siti contaminati e che preveda, a seguito di un evento potenzialmente in grado di contaminare il suolo, il sottosuolo le acque superficiali e/o le acque sotterranee:</p> <ul style="list-style-type: none"> • la comunicazione da effettuarsi alle autorità competenti al verificarsi di un evento potenzialmente in grado di contaminare o all'atto di contaminazione del suolo, del sottosuolo, delle acque superficiali e/o delle acque sotterranee, in linea con le modalità e tempistiche previste dalla normativa vigente; • l'identificazione di elementi di potenziale contaminazione (attuale o storica) ai fini della valutazione di avviamento delle necessarie attività di messa in sicurezza e di bonifica; • il monitoraggio delle procedure operative ed amministrative nel rispetto delle modalità e delle tempistiche previste dalla normativa vigente; • la verifica della realizzazione degli interventi di bonifica in linea con quanto previsto dal progetto di bonifica approvato; • la predisposizione della documentazione da presentare alle autorità competenti al completamento dell'intervento, ai fini del rilascio della certificazione di avvenuta bonifica. 		
<p>Art. 727 bis, 733 bis c.p.; art. 137 cod. ambiente; art. 8 e 9 d.lgs. 202/2007 Attività svolte su navi ed aeromobili.</p>	<p>Prevenzione e monitoraggio degli sversamenti in mare di sostanze e materiali in violazione delle normative nazionali e internazionali vigenti. Ad esempio, per le navi occorre definire ruoli, responsabilità, modalità e criteri per:</p> <ul style="list-style-type: none"> • la registrazione delle operazioni/attività che possano produrre sversamenti in mare (es. movimentazione, pulizia, ecc.); • la gestione di tali sostanze. 		
<p>Art. 256, 258 - 260 bis cod. ambiente Gestione delle attività di raccolta, caratterizzazione, classificazione e deposito dei rifiuti</p>	<p>Caratterizzazione e classificazione dei rifiuti, consistente in:</p> <ul style="list-style-type: none"> • identificazione, analisi, classificazione e registrazione dei rifiuti; • verifica rispetto ai dati dei certificati forniti dal laboratorio di analisi dei rifiuti, della corretta classificazione del rifiuto riportata nella documentazione prevista per la movimentazione dei rifiuti dalla normativa vigente. <p>Deposito temporaneo di rifiuti, prevedendo:</p> <ul style="list-style-type: none"> • la definizione dei criteri per la scelta/realizzazione delle aree adibite al deposito temporaneo 		

	<p>di rifiuti; • l'identificazione delle aree adibite al deposito temporaneo di rifiuti;</p> <ul style="list-style-type: none">• la raccolta dei rifiuti per categorie omogenee e l'identificazione delle tipologie di rifiuti ammessi all'area adibita a deposito temporaneo;• l'avvio delle operazioni di recupero o smaltimento dei rifiuti raccolti, in linea con la periodicità indicata e/o al raggiungimento dei limiti quantitativi previsti dalla normativa vigente.
<p>Art. 3 l. 549/1993 Gestione delle sostanze lesive dell'ozono.</p>	<p>Occorre prevedere modalità e criteri per:</p> <ul style="list-style-type: none">• il censimento degli <i>asset</i> contenenti sostanze lesive dell'ozono e la definizione del relativo piano dei controlli manutentivi e/o di cessazione dell'utilizzo e <i>dismissione dell'asset</i>, secondo quanto previsto dalla normativa vigente;• le verifiche periodiche di rispetto del piano ed attivazione di azioni risolutive in caso di mancato rispetto.

Art. 25-duodecies d.lgs. 231/2001 - Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare**Reato presupposto**

D.lgs. 25 luglio 1998, n. 286 (T.U. sull'immigrazione)	art. 22 comma 12 bis	Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare aggravato da: <ul style="list-style-type: none"> - numero di lavoratori irregolari superiore a tre; - impiego di minori in età non lavorativa; - sottoposizione a condizioni lavorative di particolare sfruttamento, quali l'esposizione a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.
---	-----------------------------	---

1. CONSIDERAZIONI

Il 9 agosto 2012 è entrato in vigore il d.lgs. 109/2012, il quale amplia i reati presupposto per la responsabilità amministrativa delle persone giuridiche prevista dal d.lgs. 231/2001, in attuazione della direttiva 2009/52/CE, che introduce norme relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare. È un delitto di natura dolosa, suscettibile di fondare la responsabilità dell'ente nella sola ipotesi aggravata di cui al comma 12 - *bis*.

2. AREE A RISCHIO REATO E CONTROLLI PREVENTIVI: ALCUNI ESEMPI

Aree a rischio reato	Controlli preventivi
Risorse umane/vertici aziendali, in particolare: <ul style="list-style-type: none"> • Stipulazione di contratti di lavoro subordinato (a tempo indeterminato o determinato), part-time o a tempo pieno ed autonomo; • distacco di lavoratori. 	Predisposizione di specifica procedura/check list per l'assunzione di lavoratori stranieri. Adeguato sistema di deleghe e procure in materia di assunzione dei lavoratori. Implementazione di un sistema di monitoraggio delle vicende relative ai permessi di soggiorno (scadenze, rinnovi, etc.).

Acquisti (o altre funzioni eventualmente competenti per), con particolare riferimento alla stipulazione di:

- contratti di somministrazione di lavoro;
- contratti di appalto;
- contratti d'opera.

Predisposizione di specifica procedura/check *list* per la stipula di contratti di somministrazione di lavoro, d'opera e di appalto.

Adeguate sistema di deleghe e procure in materia di stipulazione di contratti che implicano, da parte della controparte, l'impiego di forza lavoro.
Procedure autorizzative per gli acquisti.
Richiesta ai fornitori o *partner* commerciali di uno specifico impegno al rispetto della normativa in oggetto.

NOTA CONCLUSIVA

IL PRESENTE MODELLO E LE FATTISPECIE DI REATO SONO STATI EFFETTUATI IN BASE A:

- LINEE GUIDA CONFINDUSTRIA ANNO 2014
- LINEE GUIDA ANCE
- LINEE GUIDA AIAS