PARTE SPECIALE

Indice:

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 *bis***	Malversazione a danno dello Stato
	art. 316 *ter*	Indebita percezione di erogazioni a danno dello Stato
	art. 640	Truffa aggravata a danno dello Stato
	art. 640 *bis*	Truffa aggravata per il conseguimento di erogazioni pubbliche
	art. 640 *ter*	Frode informatica

1. CONSIDERAZIONI GENERALI

Il delitto di truffa aggravata in danno dello Stato è realizzabile in tutti gli ambiti operativi 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. L'ipotesi di truffa a danno dello stato o di un altro ente Pubblico appare configurabile in tutti quei casi in cui un soggetto interno all'ente svolta una attività criminosa finalizzata al rilascio di licenze, autorizzazioni o relativamente al rilascio di attestazioni per partecipazione ad una gara. Nel caso in ispecie dell'ente occorre riferirsi in particolare alle autorizzazioni e alle procedure amministrative per la presentazione della domanda di contributo al Ministero dei Beni Culturali.

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 artifizi 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 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, mediante l'utilizzo che l'Ente potrebbe farne per finalità diverse rispetto a quelle prescritte.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI:

Aree a rischio reato	Controlli preventivi
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 per l'Ente (ad es. mediante la produzione di documenti falsi attestanti l'esistenza di condizioni e/o requisiti essenziali).	Specifiche previsioni nel sistema dell'Ente di programmazione e di controllo. Puntuali attività di controllo gerarchico (incluso sistema istituzionalizzato di deleghe adozione di procedure di cui al codice degli appalti D.Lgs n. 163 e successive modifiche).

Attività 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 per l'Ente (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 modifica in via	Sistema di controlli interno all'Ente che, ai fini del corretto e legittimo accesso ai Sistemi informativi della PA, preveda: • un adeguato riscontro delle *password* di abilitazione per l'accesso ai Sistemi Informativi della PA possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche funzioni/ strutture dell'Ente; • la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dalla società; • il rispetto della normativa sulla *privacy*. Questi meccanismi assumono maggiore pregnanza per quegli 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.

informatica dei dati (es. fiscali e/o previdenziali) di interesse dell'Ente (es. modelli 770), già trasmessi alla P.A.	
Le aree maggiormente a rischio all'interno della struttura dell'Ente sono relative a: • settore delle attività finanziarie; • settore servizi amministrativi;	Specifica previsione del codice etico e diffusione di quest'ultimo tra tutti i dipendenti. 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. Separazione funzionale fra chi gestisce le attività di realizzazione e chi presenta la documentazione di avanzamento. 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'Ente che presenta il progetto). 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". 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.
Partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego. In tale contesto, assumono particolare rilevanza i seguenti ambiti di operatività: • formazione/personale; • gestione delle attività finanziarie; • settore servizi amministrativi;	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'Ente che presenta il progetto). 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. Monitoraggio sull'avanzamento del progetto realizzativo (a seguito dell'ottenimento del contributo pubblico) e sul relativo *reporting* alla PA, con evidenza e gestione delle eventuali anomalie. Controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.

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, l'Ente sarà considerato responsabile per i delitti informatici commessi a proprio 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, 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* dell'Ente e ha inciso sensibilmente sulle opportunità a disposizione di ciascun esponente dell'Ente per realizzare o occultare non soltanto schemi di condotte criminali già esistenti ma anche fattispecie nuove, tipiche del cd. *Mondo virtuale*.

A ciò si aggiunga 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 all'interno dell'Ente 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 gli Enti 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. É 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 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 (es. area amministrazione, finanza e controllo, marketing, 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'azienda[1].

Gli Enti 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 dell'Ente; *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 remoti dei dispositivi;
- l'utilizzo di sistemi di cd. *cloud computing* che prevedano, a titolo esemplificativo: *i)* la scelta dei cd. *cloud server* ammessi dall'Ente 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 dell'Ente; *iii)* la definizione e diffusione di linee guida per l'utilizzo dei servizi di *clouding* da parte di tutti gli esponenti dell'Ente.

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.

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:

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
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).	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).

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

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. Falsificazione di documenti informatici compiuta nell'ambito dei servizi di *Certification Authority* da parte di un soggetto che rilasci certificati informatici, aventi valenza probatoria, corrispondenti a false identità o attestanti falsi titoli professionali. 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).	
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. *automotive*, *design*, moda, tecnologie, ecc.). Accesso abusivo a sistemi informatici di concorrenti allo scopo di acquisire informazioni concernenti la clientela utili per esempio per l'elaborazione di strategie di *marketing* (es. dati di consumo, aree	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: • 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 dell'Ente 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

banche dati, etc.). Accesso abusivo a sistemi di enti pubblici per l'acquisizione di informazioni riservate (es. amministrazione giudiziaria o finanziaria). Accesso abusivo a sistemi interbancari al fine di modificare le informazioni sul proprio conto registrate su tali sistemi. Accesso abusivo a sistemi aziendali protetti da misure di sicurezza, per attivare servizi non richiesti dalla clientela. 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. 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. 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).	ricoperto dal soggetto (A.11.2.2, A.11.5.1 e A.11.5.2); • procedura per il controllo degli accessi (A.11.1.1); • tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici dell'ente (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).
Art. 615-*quater* c.p. Detenzione e utilizzo di *password* di accesso a siti di enti concorrenti al fine di acquisire informazioni riservate. Detenzione ed utilizzo di *password* di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse	Inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni (A.6.1.5). Procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (A.8.3.3 e A.11.2.1).

dell'ente, 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 dell'Ente 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).

attività dipende strettamente dalle infrastrutture tecnologiche, come ad esempio avviene nell'e- *commerce* o e-*banking*.	
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.	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 *software* dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema (A.10.4.1). 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).
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	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.

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 dell'Ente 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 dell'Ente 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. concessione finanziamenti agevolati per conto dei Ministeri);

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 cd. 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.

Con riferimento al delitto di corruzione "attiva", si può ipotizzare il caso in cui un dipendente dell'ente versi a un soggetto che rivesta la qualifica di Pubblico Ufficiale o incaricato di pubblico servizio, una somma di denaro al fine di ottenere una licenza, autorizzazione o altro beneficio anche in termini di contrazione dei tempi della procedura autorizzativa.

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), si pensi ad esempio ai processi civili anche in materia di lavoro, amministrativi e penali a cui partecipa o potrebbe partecipare l'Ente.

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 dell'Ente 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 dall'Ente 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, 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 dell'Ente 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'ente 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 previgente 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.

Premesso quanto sopra, si rinvia alla tabella predisposta nelle pagine seguenti, evidenziando le principali macro aree da considerarsi direttamente a rischio reato, con l'evidenziazione di alcuni possibili presidi e controlli preventivi da implementare nel contesto dell'Ente, nell'ambito di un organico sistema procedurale, ai fini della loro copertura.

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 o dell'ente, dovrà adeguarsi ai principi normativi in esso espressi. Pertanto, gli Enti Italiani 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 mutuate dal modello di organizzazione e gestione già adottato in conformità a quanto previsto dal nostro decreto 231.

In tale direzione, e del tutto parallelamente alla precedente verifica e ad una sua eventuale integrazione, appaiono indispensabili specifichi 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:

Aree a rischio reato	Controlli preventivi
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. 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. Realizzazione di accordi di *partnership* 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. Rapporti con: • Autorità Indipendenti e di Vigilanza e altri organismi di diritto pubblico; • pubblici ufficiali e incaricati di pubblico servizio relativamente agli adempimenti fiscali, tributari e previdenziali;	Monitoraggio delle offerte economiche relative a gare e a trattative private con la PA, corredato da analisi del *trend* dei prezzi praticati, nonché monitoraggio delle fasi evolutive dei procedimenti di gara o di negoziazione diretta. *Reporting* interno, a fronte delle attività di monitoraggio, per favorire sistemi di *cross control* e gestione delle anomalie tra le diverse funzioni aziendali. Procedure di tracciabilità dei flussi finanziari dell'Ente con l'individuazione dei soggetti autorizzati all'accesso alle risorse.

• Autorità Giudiziaria, pubblici ufficiali e incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale. La partecipazione a procedure per l'ottenimento di licenze, provvedimenti amministrativi ed autorizzazioni da parte della PA. Le attività di acquisto dalla PA, ovvero le attività di acquisto svolte con la qualifica di pubblica funzione o incaricato di pubblico servizio. 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. Selezione e assunzione del personale. 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.	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).
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: • consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto; • pubblicità; • sponsorizzazioni; • spese di rappresentanza; • locazioni passive; • attività di sviluppo di software e servizi ICT.	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: • 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.

Partecipazione a procedure di evidenza pubblica in associazione con altri partner (RTI, ATI, *joint venture*, consorzi, etc.).	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, occorrerà: - 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 dichiari 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 *business* (es. *joint venture*, ATI, RTI, consorzi, etc.).

Art. 25-*septies* d.lgs. 231/2001 – Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

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'ente[4], 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 nella fattispecie in oggetto, il concetto di "elusione fraudolenta" viene assunto 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'Ente 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.

---

[4] Sul punto cfr. *retro*, cap. I. modello

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).

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.

Pertanto, occorre che quest'ultimo, per essere efficacemente attuato, debba essere integrato con il "sistema" degli adempimenti dell'ente 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'ente 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 svolta;
- 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 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-*ter* c.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 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'ente in cui operano. Lo stesso può dirsi per l'impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale o allo scopo dell'ente.

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 dell'ente, 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 ente e soggetti terzi;
2. attività infragruppo, poste in essere nell'ambito dei rapporti intercorrenti fra enti appartenenti allo stesso gruppo.

Aree e attività a rischio	Controlli preventivi
Aree a rischio: • Amministrazione (in particolare, Tesoreria, Personale, Ufficio contratti/gare, ecc.) • Commerciale • Finanza • Direzione acquisiti; • Marketing[5]. **Attività** a rischio in relazione a: • rapporti con soggetti terzi: - contratti di acquisto e/o di vendita con controparti; - transazioni finanziarie con controparti; - investimenti con controparti; - sponsorizzazioni. • rapporti interni all'Ente:	Verifica dell'attendibilità commerciale e professionale dei fornitori e *partner* 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)[6]. Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni. Controlli formali e sostanziali dei flussi finanziari, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della eventuale 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 straordinarie[7]. 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.). Determinazione dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard. Identificazione di una funzione responsabile della definizione delle specifiche tecniche e della valutazione delle offerte nei contratti standard. Identificazione di un organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e

[5] 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).

[6] 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).

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.

- contratti di acquisto e/o di vendita; - gestione dei flussi finanziari;	responsabilità. Specifica previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio. 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 *market abuse*; Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

Art. 25-n*ovies* 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 *software* 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-*septies*	Violazioni nei confronti della SIAE
	art. 171-*octies*	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 dell'ente, a prescindere dall'eventuale impiego - a tal fine - di beni dell'ente (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 dell'ente, 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 dell'ente 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 dell'ente, oltre ai controlli di cui sopra, si consiglia di:

- vietare l'impiego di beni dell'ente (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 all'ente (es. sito web, 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 dell'ente, 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**
Art. 171, comma 1, lettera *a)*, l. 633/1941 *File sharing*: 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. *Upload/download*: immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche. **Art. 171, comma 3, l. 633/1941** Riproduzione, messa a disposizione, diffusione, vendita, rappresentazione di un'opera altrui non destinata alla pubblicazione.	Invito a rispettare le norme in materia di proprietà intellettuale. Controllo dei mezzi di comunicazione dell'ente. Controllo dei sistemi informatici (filtro dei siti in conferenti, regole *firewall*, controllo dei livelli di traffico, controllo dei procedimenti di *file sharing*). Divieto di impiegare beni dell'ente per adottare condotte che violino la tutela dei diritti d'autore. Clausole riferite all'osservanza delle norme in materia di proprietà intellettuale nei rapporti con i terzi contraenti.
Art. 171-*bis*, l. 633/1941 *Undelicensing*: violazioni delle condizioni di licenza di un *software.* *Hard disk loading*: vendita e relativo acquisto per l'azienda di computer sui quali sono installati *software* piratati. Utilizzazione non autorizzata di banche dati.	
Art. 171-*ter*, l. 633/1941	

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-*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 e/o aministratori*.

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.

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 strutture organizzative complesse.

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 dell'Ente;
- potere disciplinare: elemento naturalmente e spontaneamente collegato ai primi due.

2. AREE A RISCHIO E CONTROLLI PREVENTIVI:

Modalità di realizzazione del reato – attività a rischio reato	Controlli preventivi
False comunicazioni sociali – falso in prospetto 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.	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 similari, così da garantire: • massima collaborazione; • completezza e chiarezza delle informazioni fornite; • accuratezza dei dati e delle elaborazioni; • tempestiva segnalazione di eventuali conflitti di interesse. 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.) 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".

	Inoltre si suggerisce di prevedere: • 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 apposito verbale.
Impedito controllo Gli amministratori a fronte di una puntuale richiesta da parte del Collegio Sindacale in ordine al rispetto 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 rappresentare i processi	Esistenza di un sistema definito di responsabilità del vertice aziendale e di deleghe coerenti anche in tema di disciplina di *Corporate Governace.* Istituzione di riunioni periodiche tra Collegio Sindacale ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/*Corporate Governance*, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del

applicativi all'interno dell'Ente 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 l'Ente stesso.	*management* e dei dipendenti. Riporto periodico al Vertice sullo stato dei rapporti con il Collegio Sindacale e le altre Autorità abilitate ai controlli sull'ente.
Omessa comunicazione del conflitto di interessi 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.	Esistenza di un sistema definito di responsabilità del Vertice aziendale e di deleghe coerenti con esso anche in tema di disciplina di *Corporate Governace.* Identificazione delle principali fattispecie di interessi degli amministratori. Procedure autorizzative per operazioni esposte a situazioni di conflitto di interesse evidenziate da singoli amministratori.
Illecita influenza sull'assemblea 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.	Istituzione di riunioni periodiche tra Collegio Sindacale ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/*Corporate Governance* (compresa quella in tema di "parti correlate"), nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del *management*, dei dipendenti.
Aggiotaggio 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.	Tale fattispecie non rientra nell'ambito dell'Associazione

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).	Tale fattispecie non rientra nell'ambito dell'Associazione
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 verificazione di un danno per i creditori	Tale fattispecie non rientra nell'ambito dell'Associazione
Corruzione tra privati Costituiscono aree a rischio reato: • la predisposizione di bandi di gara/partecipazione a procedure competitive	Nella negoziazione e stipula di contratti attivi, devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito della negoziazione e stipula di contratti attivi prevedano:

finalizzati alla negoziazione o stipula di contratti attivi, cioè in grado di generare un ricavo per l'Ente; • 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 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.

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.	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, 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).

	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: • 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. Istituzione di una procedura per il controllo dei flussi finanziari e la tracciabilità dei pagamenti. 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. Istituzione di una procedura che garantisca il rispetto dei criteri di legalità, trasparenza, condivisione funzionale e giustificabilità nel: • 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 *target*.
Selezione, assunzione e gestione amministrativa del personale.	Adozione di uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione, assunzione e gestione amministrativa del personale prevedano: • 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 espongano 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 cosi 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.

Approvvigionamento di beni, lavori e servizi.	Previsione di procedure di autorizzazione delle richieste di acquisto e di: • 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.