PARTE SPECIALE

PROTOCOLLI E PROCEDURE

REVISIONE 1/2022

15/7/2022

SOMMARIO

PREMESSA: I PROTOCOLLI E LE PROCEDURE ADOTTATE DA MARECA

Al fine di aggiornare e implementare il sistema esistente e meglio ottemperare ai principi fissati dal D.lgs n. 231/01, Mareca s.r.l. (di seguito anche Mareca o la Società) adotta una serie di protocolli di natura preventiva in relazione alle "attività sensibili" identificate. Adotta, altresì, un sistema integrato di procedure (definite "*procedure 231*") che andrà ad essere implementato nel tempo, fornendo alla Società un ulteriore strumento di prevenzione specificamente dedicato ad alcune aree di maggior sensibilità

Dunque, al fine di rendere più efficace ed operativo il Modello, si riportano in questa parte speciale i Protocolli collegati alla prevenzione dei reati con rischio non trascurabile di commissione secondo la mappatura aggiornata ed alcune Procedure più specifiche inerenti sotto-categorie di condotte a rischio-reato.

I protocolli si fondano su una serie di criteri generali che devono trovare concreta attuazione nelle singole procedure, costituendo, altresì, il parametro di riferimento per le stesse procedure in termini d'idoneità a evitare la commissione di illeciti rilevanti ex D.lgs n. 231/01. Le procedure inserite nel Modello non esauriscono in ogni caso il complesso delle procedure specifiche adottate internamente dalla società.

Inoltre, ai fini di una più agevole verifica delle specifiche situazioni che i protocolli e procedure sono diretti a proteggere nell'ambito delle misure di prevenzione per la gestione del rischio-reato, si riporta, nell'ultima sezione di tale documento, una scheda sintetica dei cd. reati presupposto e delle principali modalità di commissione degli stessi con riferimento agli "illeciti 231" individuati, all'esito dell'aggiornamento della mappatura, quali "*reati 231 a rischio rilevante di commissione*".

Ciò premesso, è necessario richiamare alcuni criteri-guida, utilizzati poi nella descrizione dei seguenti protocolli e per la predisposizione delle specifiche procedure operative:

- il sistema organizzativo delle diverse aree di attività deve essere chiaro e cioè adeguatamente formalizzato e conosciuto sia in relazione all'attribuzione dei poteri – deleghe, sia con riferimento all'individuazione delle dipendenze gerarchiche;
- le responsabilità devono essere definite e debitamente distribuite, evitando, per le attività sensibili, sovrapposizioni ovvero attribuzioni ad un unico soggetto di determinati poteri creando situazioni in cui un processo sia interamente gestito da una sola persona; è necessario assicurare opportuni punti di controllo;
- i poteri di rappresentanza e di firma, nonché quelli relativi all'autorizzazione per determinate attività, devono essere conferiti nell'ambito dell'esercizio delle mansioni effettivamente assegnate;
- il sistema di deleghe (e cioè l'atto interno mediante il quale sono attribuiti mansioni, compiti e funzioni) e di procure (ossia, l'atto di natura negoziale che conferisce il potere di rappresentanza di Mareca nei confronti dei terzi) devono rispondere ai seguenti requisiti:
    - ✓ ogni delega deve contenere in modo chiaro ed esaustivo l'indicazione dei poteri delegati, il soggetto cui riporta gerarchicamente, il potere di spesa eventualmente conferito, il quale deve essere adeguato all'incarico attribuito;
    - ✓ la procura può essere generale o speciale: nel primo caso, deve comunque contenere la descrizione dei poteri attribuiti in relazione alle diverse attività aziendali, nonché l'indicazione del potere di spesa; nel secondo caso, la procura deve contenere in modo preciso l'oggetto dell'incarico per cui è rilasciata, con la specificazione dei poteri che, ad ogni modo, devono essere conferiti solo in relazione all'incarico in questione;
    - ✓ sia le deleghe che le procure devono essere tempestivamente adeguate in relazione ai cambiamenti interni societari;
    - ✓ tutti i soggetti che operano per conto di Mareca con la Pubblica Amministrazione devono essere dotati formalmente di delega o di procura;
- i protocolli e le procedure non devono in alcun modo contrastare con il contenuto del Codice Etico e, inoltre, sono predisposti, ed attuati, prevedendo:
- la separazione dei ruoli, tenendo conto della specifica attività o del settore coinvolto e dell'importanza della procedura, tra il soggetto che ha il potere decisionale, quello che ne cura gli aspetti operativi e quello che opera il controllo;
- la tracciabilità scritta per le diverse fasi della procedura;

- la formalizzazione della procedura al fine di premetterne la conoscibilità e la corretta esecuzione e di agevolare l'attività di controllo;
- la possibilità di effettuare controlli a campione durante la fase esecutiva, oltre agli ordinari controlli che devono consentire l'individuazione e la segnalazione tempestiva di eventuali anomalie;
- i protocolli e le procedure devono essere oggetto di adeguata comunicazione e formazione rispetto ai destinatari.

Con riferimento alle specifiche attività sensibili identificate in relazione alle attività condotte, in particolare visite presso la Società ed interviste a dipendenti e organi apicali, sono stati adottati i seguenti protocolli e procedure che costituiscono a tutti gli effetti norme comportamentali vincolanti, la cui violazione è da considerarsi illecito disciplinare da sanzionare ai sensi e per gli effetti del regolamento sanzionatorio previsto dal Modello organizzativo.

A. PROTOCOLLI

A.1. REGOLE DI COMPORTAMENTO NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

I contatti, diretti e indiretti, tra la Società e la Pubblica Amministrazione costituiscono un'area sensibile con riferimento alla possibilità di commissione di varie tipologie di illeciti previsti dal Decreto.

Il Protocollo qui disciplinato funge da regola generale e da prescrizione vincolante nei rapporti con la Pubblica Amministrazione, indicando i criteri di comportamento che devono essere scrupolosamente osservati.

Il concetto di Pubblica Amministrazione va qui inteso in senso estensivo, comprensivo di enti pubblici economici, enti sottoposti a vigilanza ministeriale (tra cui, a titolo di esempio: AST, Agenzia delle Entrate, Camera di commercio), organismi di diritto pubblico o privati con finalità pubblica ed eroganti fondi di natura pubblica (ad esempio "Fondimprese" o similari).

Rapporti con enti o funzionari pubblici italiani

- I rapporti con la Pubblica Amministrazione sono improntati a criteri di trasparenza e professionalità, in uno spirito di massima collaborazione e nel rispetto dei principi fissati nel Codice Etico.
- Tali rapporti sono intrattenuti dalle varie funzioni aziendali a ciò preposte a seconda dell'importanza e della rilevanza della problematica di volta in volta in rilievo; le varie funzioni aziendali coinvolte redigono relazioni o rapporti scritti sullo stato delle varie pratiche che devono essere archiviati e messi a conoscenza dei responsabili in via gerarchica.
- La redazione dei suddetti rapporti può essere periodica o può avvenire anche a seguito di singoli incontri con la Pubblica Amministrazione in relazione

all'importanza e allo stato della pratica. In ogni caso, è fatto obbligo di segnalare eventuali situazioni anomale che determinino una variazione nell'iter amministrativo rispetto alle normali prassi. Le relazioni o i rapporti vanno compilati e conservati nell'archivio di ciascuna pratica.

- Quando è in corso qualsiasi trattativa, richiesta o rapporto con la Pubblica Amministrazione, il personale incaricato non deve cercare di influenzare impropriamente le decisioni dei funzionari che trattano o prendono decisioni per conto della Pubblica Amministrazione, né tanto meno porre in essere, direttamente o indirettamente, azioni quali:
  - ✓ esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione a titolo personale;
  - ✓ sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti al di fuori di quanto consentito dalla legge;
  - ✓ ogni richiesta di contributi, finanziamenti o altre erogazioni concessi o erogati dallo Stato, da altri enti pubblici e dalle Comunità europee deve essere preventivamente autorizzata dall'Amministratore, che ne deve verificare la corrispondenza alle norme di legge;
  - ✓ ogni flusso di denaro erogato dalla Pubblica Amministrazione e la provenienza e la destinazione di tali somme devono essere adeguatamente giustificati e devono essere portati a conoscenza dell'Organismo di Vigilanza;
  - ✓ qualora nei rapporti intercorrenti con la Pubblica Amministrazione siano necessari degli esborsi da parte della Società, tali operazioni dovranno essere preventivamente sottoposte ad autorizzazione dell'Amministratore, che ne deve verificare la corrispondenza alle norme di legge e ai regolamenti aziendali;
  - ✓ chiunque venga a conoscenza di qualsiasi forma di violazione ai presenti precetti, deve prontamente informare l'Organismo di Vigilanza;
  - ✓ effettuare attività di mediazione, sfruttando o vantando asseriti o esistenti rapporti con pubblici ufficiali, ovvero ponendo in essere condotte che violino i principi di trasparenza e onestà di cui al Codice Etico;

Rapporti con enti pubblici produttori di servizi economici sottoposti a vigilanza ministeriale

- I rapporti con tali enti pubblici sono improntati a criteri di trasparenza e professionalità, in uno spirito di massima collaborazione e nel rispetto dei principi fissati nel Codice Etico.
- Considerata la peculiare forma giuridica degli enti pubblici, che agiscono nella forma di Agenzie sottoposte a poteri di vigilanza ministeriali, la Società potrebbe richiedere contributi e finanziamenti attraverso apposita domanda pubblica di partecipazione per il tramite del suo legale rappresentante pro tempore, che è subordinata in ogni caso alla assegnazione dei relativi Fondi da parte del Ministero competente.
- Ogni richiesta di contributi o finanziamenti alle Agenzie è valutata sulla base del loro regolamento interno, le delibere del CdA di tali Agenzie, le Linee Guida Ministeriali per concessione dei contributi emanate per specifica area di disciplina.
- Ogni domanda di contributo, che deve essere formalmente presentata e sottoscritta dal Legale Rappresentante di Mareca (con l'indicazione del Referente Operativo), deve contenere documentazione di cui il beneficiario conferma, assumendone la piena responsabilità, la veridicità e autenticità.
- Il soggetto beneficiario si obbliga a realizzare le azioni contenute nel progetto presentato e a presentare, qualora sia richiesto, una fideiussione bancaria o assicurativa pari all'importo dell'anticipo concesso, comprensiva della copertura del rischio di mancata o incompleta realizzazione del progetto.
- Mareca deve impegnarsi a mantenere, per tutta la durata del procedimento autorizzativo, le condizioni richieste per la concessione del contributo (la cui sussistenza viene verificata tramite possibili ispezioni e controlli).
- Nella domanda di partecipazione deve dare atto che il progetto da finanziare non è oggetto di specifici protocolli di intesa o convenzioni sottoscritti con enti pubblici o con organismi, enti e società a prevalente capitale pubblico, da cui derivano finanziamenti per la realizzazione del medesimo progetto.

- La richiesta di contributo viene effettuata attraverso il formulario apposito con contenuto operativo e di spesa del progetto richiesto.
- Ai fini dell'accesso al contributo la Società si impegna e si obbliga (e ne dà comunicazione nella domanda) ad aver adempiuto e ad adempiere agli obblighi fiscali e in materia di salute e sicurezza sul lavoro e non essere soggetto a procedimenti o condanne penali ai sensi della Legge Nazionale e della Direttiva 2014/24/UE.
- L'operatore economico non deve trovarsi in una situazione di conflitto di interesse legato alla sua partecipazione alla procedura di appalto (e in cado contrario lo deve dichiarare nella domanda di partecipazione, così agendo in condizioni di massima trasparenza).
- L'operatore economico (o soggetto collegato) non deve aver fornito o fornire consulenza all'amministrazione aggiudicatrice o all'ente aggiudicatore o altrimenti partecipare alla preparazione della procedura di aggiudicazione (in caso contrario fornendo informazioni dettagliate sulle misure adottate per prevenire le possibili distorsioni della concorrenza).
- In caso di accettazione della richiesta di contributo, Mareca realizza il progetto rispettando l'importo di spesa coperto dal contributo, non sostenendo le spese ritenute non ammissibili dal committente.
- Di tutti i rapporti deve essere informato l'Organismo di Vigilanza.
- Chiunque venga a conoscenza di qualsiasi forma di violazione ai presenti precetti, deve prontamente informare l'Organismo di Vigilanza.
- I contributi di ogni genere sono immessi con apposito capitolo sulla procedura di fatturazione dei contributi ed apposita postazione a bilancio.
- Il soggetto beneficiario si obbliga qualora sia richiesto, ad aprire un conto dedicato all'operazione del progetto.
- La procedura sopradescritta può essere anche oggetto di apposita richiesta e procedura assentiva da parte di particolari soggetti di riferimento, nel caso della Società, ad esempio, di IKEA s.p.a., che per le loro caratteristiche e per il legame con procedure specifiche interne o trasnazionali, sono assimilabili a soggetti pubblici.

Rapporti con enti o funzionari pubblici di Stati stranieri

Per quanto concerne i rapporti con la Pubblica Amministrazione di Stati esteri, il responsabile del progetto deve effettuare gli opportuni accertamenti, dando evidenza scritta degli esiti riscontrati, in relazione ai seguenti aspetti:

- valutazione in via preventiva del livello di corruzione nella pubblica amministrazione dello Stato interessato al fine di verificare, attraverso gli indici internazionalmente riconosciuti (CPI, Corruption Perception Index e BPI, Bribe Payers Index), il cd. "rischio paese";
- identificazione in via preventiva gli uffici pubblici stranieri che sono coinvolti nell'iniziativa;
- individuazione e acquisizione della documentazione relativa a esperienze precedenti nello Stato estero interessato;
- inoltre, devono essere individuati, in via preventiva e attraverso un atto formale, i soggetti che per conto della Società gestiscono i rapporti con i funzionari pubblici stranieri, ivi compresi i professionisti esterni;
- deve essere scadenzata un'attività di reporting sull'andamento dell'iniziativa, sia in fase di preparazione che in fase di resoconto che verrà inviata all'Amministratore ed all'Organismo di Vigilanza;
- deve essere preventivamente fissato un budget dettagliato in relazione alla singola iniziativa ed ogni scostamento rilevante dallo stesso deve essere giustificato per iscritto con comunicazione all'Amministratore Unico ed al Collegio Sindacale, se nominato, e deve essere identificata l'area che si occupa della singola iniziativa e la funzione cui si riporta.

L'attività di mediazione con i funzionari esteri non può essere compiuta sfruttando o vantando asseriti o esistenti rapporti con pubblici ufficiali, ovvero ponendo in essere condotte che violino i principi di trasparenza e onestà di cui al Codice Etico;

L'organismo di vigilanza deve essere informato, in dettaglio e per iscritto, delle iniziative assunte all'estero da Mareca anche al fine del controllo dell'effettivo svolgimento delle suddette attività propedeutiche.

A.2. REGOLE PER LA GESTIONE DEL RAPPORTO CON I CONSULENTI E PROFESSIONISTI ESTERNI IN CONTATTO CON LA P.A.

- Qualora Mareca utilizzi un "soggetto terzo" per essere rappresentata nei rapporti con la Pubblica Amministrazione, dovrà essere espressamente previsto nella lettera di incarico o nel contratto di collaborazione che nei confronti del consulente valgono le medesime regole di condotta e principi fissati per il personale dipendente nel Modello e nel Codice Etico.
- Ad ogni modo, la Società non potrà farsi rappresentare da "soggetti terzi" che possano trovarsi in situazioni di conflitto di interesse.
- La funzione aziendale che ravvisasse la necessità della nomina di un consulente provvede a segnalare all'Amministratore le esigenze alla base della nomina del consulente. Se poi la funzione aziendale è già orientata verso l'individuazione di uno specifico consulente, indica anche il nominativo del consulente.
- L'Amministratore esamina la richiesta della nomina del consulente, il nominativo o i nominativi proposti, provvede alla nomina del consulente.
- L'Amministratore è incaricato, con facoltà di delega, di negoziare e di stipulare il contratto con il consulente e provvede a conservare e raccogliere tutta la documentazione relativa all'incarico attribuito.
- Il contratto non potrà essere validamente concluso qualora il consulente rifiuti di sottoscrivere espressamente le clausole relative al rispetto è principi fissati dal Codice Etico. Tale documento è messo a disposizione del consulente prima della stipulazione del contratto.
- Il contratto deve specificare l'oggetto, i poteri, il compenso e - ove possibile - la durata.
- Il compenso del consulente deve essere determinato sulla base delle rispettive tabelle professionali e deve rispettare le indicazioni del budget fissato per la specifica commessa (o le diverse commesse) per cui è chiamato a prestare la propria attività. Eventuali scostamenti devono essere autorizzati per iscritto dall'Amministratore.

- Qualora la nomina del consulente comportasse una spesa non prevista dal relativo budget, la decisione sulla nomina del consulente è adottata dall'Amministratore. A tal fine l'Amministratore compila una relazione scritta con le esigenze alla base della nomina del consulente, il profilo professionale dell'eventuale candidato, il compenso complessivo proposto o negoziato e le eventuali preferenze;
- qualora l'oggetto della consulenza sia riferibile ad attività di mediazione, è fatto divieto assoluto effettuare tale attività, sfruttando o vantando asseriti o esistenti rapporti con pubblici ufficiali, ovvero ponendo in essere condotte che violino i principi di trasparenza e onestà di cui al Codice Etico.
- Il soggetto beneficiario si obbliga qualora sia richiesto dalla normativa, ad aprire un conto dedicato all'operazione del progetto e si ricorda che la legge ha introdotto le disposizioni in tema di tracciabilità dei flussi finanziari per contrastare la criminalità organizzata e le infiltrazioni nelle commesse pubbliche, e quindi è da osservare il meccanismo di anticipare la soglia di prevenzione, creando meccanismi che consentano di intercettare i fenomeni di intrusione criminale nella contrattualistica pubblica e rendere trasparenti le operazioni finanziarie relative all'utilizzo del corrispettivo dei contratti pubblici, in modo da consentire un controllo a posteriori sui flussi finanziari provenienti dalle amministrazioni pubbliche.

A.3. REGOLE IN MATERIA DI GESTIONE DEGLI OMAGGI

Con riferimento alla natura promozionale dell'attività svolta, Mareca ha inteso adottare specifiche regole per quanto concerne la gestione degli omaggi, al fine di evitare che possano configurare, anche solo in via ipotetica, occasione di commissione di illeciti rilevanti ex D.lgs n. 231/01.

Nello specifico, sono fissate le seguenti regole di natura comportamentale.

- Non è consentito offrire denaro o doni a dirigenti, funzionari o dipendenti della Pubblica Amministrazione o di enti concessionari di un pubblico servizio o a loro parenti, sia italiani che di altri paesi, nonché a soggetti stranieri che per le leggi italiane siano da considerare pubblici ufficiali, salvo che si tratti doni o utilità d'uso di modico valore.
- Al fine di evitare interpretazioni non coerenti o dettate da eccessiva discrezionalità, l'Amministratore stabilisce con delibera il valore massimo da considerarsi importo di "modico valore" e individua e adotta le procedure con cui tali importi e/o utilità possono essere erogati.
- Nello specifico, tali procedure devono garantire il massimo rispetto dei principi di trasparenza e di tracciabilità di ogni singola operazione e devono prevedere la specifica autorizzazione dell'Amministratore ogni qualvolta vengano derogati i limiti e le regole stabilite.
- Il Protocollo qui disciplinato si estende altresì ai "soggetti terzi" di cui la Società si avvale per essere rappresentata nei rapporti con la Pubblica Amministrazione.
- In ogni caso tali omaggi non devono in alcun modo poter essere considerati come volti ad acquisire vantaggi in modo improprio.
- Per parte loro i Dipendenti e tutti i soggetti che operano per perseguire gli interessi della Società non devono accettare doni o prestazioni di qualsiasi natura da soggetti con i quali intrattengono rapporti connessi con la propria attività lavorativa, se questi eccedono i limiti previsti dalle consuetudini o se sono in ogni caso contrari alla normativa attualmente in vigore. A tal fine ciascun dipendente o collaboratore si impegna a non accettare o restituire gli omaggi ricevuti.
- Nei Paesi in cui è prassi accertata e notoriamente diffusa l'offerta di doni a terzi soggetti, è possibile agire in tal senso quando questi doni siano di natura

appropriata e di valore modico e sempre nel rispetto delle leggi. Ciò non deve comunque mai essere interpretato come una ricerca di favori.

- Di ogni omaggio che esorbiti come valore dalle procedure e dai criteri ordinari effettuato a soggetti facenti parte della Pubblica Amministrazione o ad altri soggetti "privati" deve essere data tempestiva comunicazione all'Organismo di Vigilanza.
- Chiunque venga a conoscenza di qualsiasi forma di violazione ai presenti precetti, deve prontamente informare l'Organismo di Vigilanza.

Mareca indica in una apposita voce formante il proprio bilancio una posta per eventuali omaggi e la documentazione delle operazioni ed il sistema di controllo interno (contabile ed amministrativo) della Società: a) devono garantire la piena tracciabilità dalle fonti delle risorse aziendali e devono consentire la corretta ed immediata identificazione per responsabilità e natura delle prestazioni effettuate dalla loro origine sino al corretto e documentato impegno delle risorse aziendali; b) devono consentire la corretta identificazione per responsabilità, natura e destinazione degli investimenti e dei costi sostenuti dalla loro origine sino alla regolarità del relativo pagamento e il conseguente corretto e documentato utilizzo delle risorse aziendali;

A. 4. REGOLE IN MATERIA DI SELEZIONE E GESTIONE DEL PERSONALE

Il processo di selezione del personale si applica per tutti i segmenti professionali di interesse e deve rispondere ai criteri di tracciabilità e registrazione di ogni operazione.

Nello specifico, vengono fissati i seguenti criteri guida:

- la selezione di una risorsa si colloca all'interno di un processo di pianificazione delle risorse da assumere che tiene conto del fabbisogno con l'individuazione, ove possibile, 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;
- il processo di selezione si attiva mediante (i) la ricerca di una pluralità di candidature in funzione della complessità del ruolo da ricoprire e garantendo sempre la tracciabilità delle fonti di reperimento dei CV (ad es. società di head-hunting e recruitment, inserzioni, domande spontanee, presentazioni interne etc.); (ii) la verifica e la gestione dei conflitti di interesse tra il selezionatore e il candidato; (iii) la verifica, attraverso diverse fasi di screening, della coerenza delle candidature con il profilo definito; (iv) 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);
- l'autorizzazione all'assunzione viene rilasciata da parte degli adeguati livelli organizzativi e l la sottoscrizione del contratto è effettuata da persona munita da adeguati poteri di rappresentanza;
- la selezione di ciascuna risorsa deve essere documentata e la relativa documentazione deve essere conservata dal responsabile del settore HR.

La gestione del personale avviene nel rispetto delle normative di settore vigenti e in accordo con i principi fissati nel Codice Etico.

In particolare, viene garantita:

- la necessaria attività di informazione e formazione rispetto alla mansione assegnata, alla struttura organizzativa ed ai riferimenti gerarchici;
- la necessaria attività di informazione e formazione con riferimento al Modello organizzativo ex D.lgs 231/01 ed al suo funzionamento, al Codice Etico di della Società ed altre norme e regole in materia di prevenzione dei reati;
- l'adozione di modalità di gestione dall'anagrafica, delle presenze e dei dati personali in ottemperanza alla disciplina di settore;
- l'adozione di un sistema di verifica della correttezza delle retribuzioni erogate e della gestione di premi e bonus.
- i candidati dovranno specificare se essi o un parente entro il secondo grado è attualmente un dipendente della Pubblica Amministrazione o se è un ex dipendente della Pubblica Amministrazione italiana o estera. Con riferimento ad entrambe le ipotesi dovrà specificare se, nello svolgimento della sua attività, partecipi o abbia partecipato personalmente ad attività della Pubblica Amministrazione riguardanti la società, vagliato richieste effettuate dalla Società (p.es. concessioni di contributi o verifica di rendicontazioni) o la posizione della Società medesima in relazione ad un adempimento di legge; b) essi o loro familiari hanno cointeressenze in attività concernenti la posizione di fornitori, clienti, concorrenti, finanziatori o soci. Analoga condizione dovrà essere specificata con riferimento alla posizione dei parenti ed affini entro il secondo grado. Tale documentazione dovrà essere conservata nel fascicolo personale.
- In caso di dichiarazione di conflitto di interessi, non è possibile procedere all'assunzione senza il consenso dell'Organo Amministrativo, dandone avviso all'Organismo di Vigilanza.

A.5. REGOLE PER IL CONTROLLO DI GESTIONE

Mareca ha procedimentalizzato, anche attraverso un sistema informatico e l'intervento di diverse funzioni a scopo di controllo incrociato, le fasi che caratterizzano il "controllo di gestione" così ponendo in essere misure di carattere organizzativo e procedurale idonee ad evitare l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non veritieri, ancorché attraverso l'omissione nei suddetti documenti di informazioni, la cui comunicazione è imposta dalla legge, riguardo alla situazione economica, patrimoniale o finanziaria.

In particolare, Mareca ha formalizzato regole precise per la corretta e trasparente redazione del budget economico e del bilancio aziendale, individuando le responsabilità e i controlli richiesti.

Il processo di budget:

- La fase che dà avvio alla relazione del budget è espletata dal Responsabile amministrativo che deve raccogliere le necessarie fonti informative: il piano degli investimenti, il budget economico dell'esercizio in corso, i preconsuntivi di chiusura della gestione in corso e le proposte di budget elaborate dai Responsabili di Funzione.
- Successivamente, unitamente alla Direzione, il Responsabile Amministrativo analizza e verifica la congruenza delle informazioni raccolte nelle proposte di budget, tenendo in debita considerazione gli obiettivi strategici di medio periodo.
- La Direzione Amministrativa poi formalizza il budget economico complessivo suddiviso per mesi e provvede a validare il budget economico.
- Con cadenza periodica, la funzione amministrativa è incaricata, inoltre, tramite l'analisi di report periodici gestionali, di confrontare le stime a budget dei costi e ricavi con quelli effettivamente sostenuti nel periodo.
- In occasione dei suddetti momenti di verifica la direzione confronta le stime a budget dei costi e ricavi con quelli effettivamente sostenuti nel periodo, analizzandone gli eventuali scostamenti e applicando tempestivamente le azioni correttive, eventualmente effettuando una ri-previsione del budget
- Evitare che la funzione amministrativa anche con propri diretti collaboratori non assolva alla richiesta di informazioni utili al controllo sugli atti di indirizzo e governo dell'Azienda da parte di soci, o che altri organi sociali o della società di revisione

mediante l'occultamento della documentazione necessaria al controllo stesso ad esempio, attraverso l'esibizione parziale o alterata di detta documentazione.;

A.6. REGOLE IN MATERIA DI PREDISPOSIZIONE DEL BILANCIO

Il processo di redazione del bilancio è condotto attraverso una prima fase di analisi e controllo, eseguita con periodicità trimestrale anche nel corso dell'esercizio, delle seguenti voci:

- ciclo passivo e ciclo attivo a cura dell'ufficio amministrativo - contabilità generale;
- conti patrimoniali del personale a cura dell'ufficio del personale e dell'ufficio amministrativo - contabilità generale per quanto di competenza;
- finanza a cura dell'ufficio amministrativo - contabilità generale.

Successivamente vengono effettuate le previsioni dei costi e dei ricavi di competenza dell'esercizio sulla base dei contratti in essere, degli ordini emessi e dei dati storici.

Entro un congruo periodo antecedente l'assemblea sociale l'Amministratore presenta la proposta di bilancio aziendale con il consulente fiscale.

Le ulteriori attività da espletare per arrivare all'approvazione del bilancio sono le seguenti:

- trasmissione del bilancio d'esercizio al Collegio sindacale se nominato, entro il giorno successivo all'approvazione del bilancio per la stesura dell'apposita relazione;
- convocazione dell'Assemblea dei soci da parte del Presidente entro il termine statutario per l'approvazione del bilancio aziendale da parte dell'Assemblea dei soci stessa.
- Esiste la possibilità che in documenti contabili dell'Azienda o in altri documenti contenenti comunicazioni sociali dirette ai portatori di interesse vengano determinate poste valutative di bilancio non conformi alla reale situazione dell'Azienda oppure vengano esposti fatti non veri o vengano omesse informazioni dovute riguardo all'Azienda.
- Sono da impedire attestazioni false o di nascondere informazioni riguardo alla situazione dell'Azienda per avvantaggiarla. ·

A.7. REGOLE IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

Il presente Protocollo riguarda i reati previsti dall'articolo 25-septies del D.Lgs. n. 231/01 (di seguito, per brevità, i "Reati in materia di salute e sicurezza sul lavoro").

In questa sede è opportuno ricordare che il decreto legislativo n. 81 del 2008 (Testo Unico in materia di Sicurezza ed igiene del lavoro, di seguito, per brevità, il "TUS") ha stabilito un contenuto minimo essenziale del modello organizzativo in questa materia. L'articolo 30 del TUS, infatti, dispone che:

"Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e

protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di

lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il

mancato rispetto delle misure indicate nel modello. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico…"

In tema di reati in materia di salute e sicurezza sul lavoro, l'art. 25-septies del Decreto, prevede e regolamenta i casi di "*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*".

Principi e regole generali

Nell'ambito del presente Protocollo vengono riportati i principi di comportamento che si richiede vengano adottati da parte di tutto il personale aziendale nello svolgimento di tutte le attività attinenti alla normativa sulla salute e la sicurezza sul lavoro. Tali regole di condotta sono finalizzate a limitare il più possibile il verificarsi dei reati previsti nel Decreto.

I principi di comportamento si applicano direttamente a chiunque sia tenuto, in via diretta od indiretta, all'osservanza delle norme antinfortunistiche. La normativa vigente individua i seguenti soggetti quali garanti ex lege, per quanto di rispettiva competenza, dell'obbligo di sicurezza: datore di lavoro, dirigenti, preposti, lavoratori.

In particolare, sono indelegabili da parte del datore di lavoro i seguenti obblighi previsti ex art. 17, TUS:

- la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 29 TUS;
- la designazione del responsabile di prevenzione e protezione dai rischi.

Fatta eccezione per quanto stabilito dall'art. 17, TUS attraverso lo strumento della delega di funzioni previsto dall'art. 16, TUS, il datore di lavoro può delegare, nel rispetto delle condizioni dettate dall'art.16, TUS, l'esecuzione degli obblighi di sicurezza a soggetti che siano dotati delle necessarie competenze. I soggetti delegati dal datore di lavoro possono a loro volta subdelegare l'esecuzione degli obblighi di sicurezza nei limiti previsti dall'art. 16, comma 3-bis TUS.

Datore di lavoro e dirigenti sono tenuti all'adempimento degli obblighi previsti dall'articolo 18 TUS, nel quadro della più ampia previsione dell'art. 2087 cc, qualificata quale norma di chiusura del sistema con riferimento alla portata dell'obbligo di sicurezza posto ex lege in capo al datore di lavoro.

In particolare, datore di lavoro e dirigenti sono tenuti a vigilare sull'adempimento degli obblighi di sicurezza posti dalla normativa in capo a preposti, lavoratori, progettisti, fabbricanti, fornitori, installatori e medici competenti.

Gli obblighi di sicurezza posti dalla normativa vigente in capo a preposti e lavoratori sono compiutamente disciplinati rispettivamente dagli articoli 19 e 20 TUS.

In base al disposto dell'articolo 31 TUS il datore di lavoro organizza il servizio di prevenzione e protezione all'interno dell'azienda o dell'unità produttiva, o incarica persone o servizi esterni, in assenza di dipendenti che all'interno dell'azienda ovvero dell'unità produttiva, siano in possesso delle capacità e dei requisiti professionali di cui all'articolo 32, TUS.

Il presente Protocollo prevede l'espresso divieto, per tutti i Destinatari del Modello adottato da Mareca di:

- porre in essere comportamenti tali da integrare fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del Decreto);
- porre in essere comportamenti imprudenti, negligenti od imperiti che possano costituire un pericolo per la sicurezza all'interno dei luoghi di lavoro;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- rifiutare di utilizzare dispositivi di protezione individuale o collettivi, ove previsti, o svolgere attività lavorative in violazione delle disposizioni impartite dai responsabili per la sicurezza;
- svolgere attività di lavoro e adoperare macchinari e strumentazioni senza aver
- preventivamente ricevuto adeguate istruzioni sulle modalità operative oppure senza aver precedentemente partecipato a corsi di formazione;
- omettere la segnalazione della propria eventuale incapacità o inesperienza nell'uso di strumenti aziendali;

- rifiutarsi di partecipare a corsi di formazione in materia di salute e sicurezza sul luogo di lavoro.
- Sotto l'aspetto generale, nell'ambito dei suddetti comportamenti i soggetti aziendali preposti all'attuazione delle misure di sicurezza - ciascuno per le attività di sua competenza specificamente individuate - sono tenuti ad assicurare:
    - il rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti e luoghi di lavoro;
    - l'attuazione delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
    - l'attuazione di modifiche di natura organizzativa finalizzate a far fronte a emergenze, primo soccorso, gestione degli appalti;
    - il corretto svolgimento delle riunioni periodiche di sicurezza e delle consultazioni dei rappresentanti dei lavoratori per la sicurezza;
    - le attività di sorveglianza sanitaria;
    - le attività di formazione e informazione del personale;
    - le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte del personale;
    - l'acquisizione della documentazione e delle certificazioni obbligatorie di legge;
    - le verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

Al fine di garantire un'adeguata gestione della sicurezza sul lavoro, la Società provvede a predisporre:

1) idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui ai precedenti punti da a) ad i);

2) un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello, secondo i dettami stabiliti dalle normative vigenti;

3) un idoneo sistema di controllo sull'attuazione degli obiettivi prefissati in materia di sicurezza e del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative

delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

4) l'esistenza di un documento di politica interna, diffuso tra i dipendenti, che stabilisca gli indirizzi e gli obiettivi generali del sistema di prevenzione e protezione volti a perseguire obiettivi in materia di salute e sicurezza.

Il budget dei piani annuali e pluriennali degli investimenti e di programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza.

Il presente Protocollo prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni o omissioni, conformemente alla loro formazione ed alle istruzioni e ai mezzi forniti dal Datore di Lavoro ai fini sicurezza;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro ai fini sicurezza, dai dirigenti e dai soggetti preposti alla sicurezza ai fini della protezione collettiva e individuale;
- utilizzare correttamente i macchinari e le apparecchiature, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
- segnalare immediatamente al Datore di Lavoro ai fini sicurezza, al Servizio di Prevenzione e Protezione ed agli altri soggetti coinvolti nel sistema di gestione della sicurezza malfunzionamenti dei mezzi e dispositivi di cui ai punti che precedono, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali malfunzionamenti o pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti;
- contribuire, insieme al Datore di Lavoro, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

In generale tutti i Destinatari del Modello devono rispettare quanto definito al fine di preservare la sicurezza e la salute dei lavoratori e comunicare tempestivamente alle strutture interne competenti eventuali segnali di rischio e/o pericolo, incidenti

(indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e delle procedure aziendali.

É fatto divieto ai Destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare, presi individualmente o collettivamente, in maniera diretta o indiretta, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del Decreto).

É fatto, altresì, divieto di porre in essere comportamenti in violazione dei principi e delle Procedure aziendali previste nel presente Protocollo, ovvero ad altre disposizioni aziendali in materia di salute e sicurezza dei luoghi di lavoro.

In particolare, con riferimento ai Terzi:

- gli appaltatori devono: (i) garantire la propria idoneità tecnico-professionale con riferimento ai lavori da eseguire; (ii) recepire le informazioni fornite dalla Società in merito ai rischi presenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate dalla Società; (iii) cooperare e coordinare con la Società per l'individuazione e l'attuazione delle misure di prevenzione e protezione e degli interventi necessari al fine di prevenire i rischi sul lavoro a cui sono esposti i soggetti coinvolti, anche indirettamente, nell'esecuzione dei lavori da eseguire in appalto o mediante contratto d'opera o di somministrazione;
- i fornitori devono vendere, noleggiare e concedere in uso esclusivamente strumenti ed attrezzature di lavoro, dispositivi di protezione individuali ed impianti che siano conformi alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro;
- gli installatori, infine, devono attenersi alle istruzioni fornite dai fabbricanti dei prodotti da installare, con particolare riferimento alle misure e agli adempimenti in materia di salute e sicurezza sul lavoro.

Al fine di consentire all'Organismo di Vigilanza l'effettuazione dell'attività di monitoraggio della funzionalità del sistema preventivo adottato con riferimento all'ambito della salute e sicurezza sul lavoro, deve essere messa a disposizione dello stesso Organismo copia della reportistica periodica in materia di salute e sicurezza sul lavoro, del verbale della riunione periodica di cui all'art. 35 del D. Lgs. 81/08, nonché tutti i dati relativi agli infortuni sul lavoro occorsi.

Eventuali violazioni delle norme in materia di salute e sicurezza sul lavoro ed in particolare delle prescrizioni contenute nelle regole aziendali (incluso il presente Modello) devono essere sanzionate, nel rispetto di quanto previsto dalla legge e dalla contrattazione collettiva, in accordo a quanto disciplinato nel Sistema Sanzionatorio e Disciplinare.

La Società ha facoltà di integrare, in qualsiasi momento, i principi elencati nel presente paragrafo così come le procedure aziendali vigenti, qualora ritenuto opportuno al fine di garantire la salute e sicurezza sul lavoro

A.8. REGOLE IN MATERIA DI PREVENZIONE DEI DELITTI INFORMATICI

Il presente protocollo stabilisce il divieto generale di

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato di cui all'art. 24-bis del Decreto;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Il protocollo prevede, conseguentemente, l'obbligo a carico dei Destinatari di accedere al sistema attraverso specifiche misure di autenticazione e autorizzazione informatica, nonché tenere condotte atte a garantire la sicurezza dei dati trattati, il rischio di distruzione o di perdita ed il rischio di accesso non autorizzato o non consentito.

È consigliata la predisposizione, da parte dell'Ufficio IT e di una società esterna, di un disciplinare tecnico più specifico (procedure) in materia di misure minime di sicurezza informatica, da divulgare a tutti i dipendenti della società.

Le regole generali di seguito individuate sono poste a carico di tutti i destinatari del Modello 231 che operano attraverso sistemi informatici e i controlli richiesti sono effettuati dall'Ufficio IT, opportunamente coadiuvato, ove necessario, da una società esterna di consulenza informatica.

Nello specifico, è opportuno:

- tenere un comportamento corretto, trasparente e collaborativo in tutte le attività finalizzate alle comunicazioni sociali;

- assicurare un pieno rispetto delle norme di legge e regolamenti, nonché delle procedure aziendali interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni anche per finalità di legge;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche con particolare attenzione a quelle destinate all'Autorità Garante della Privacy, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;
- predisporre efficaci piani di sicurezza e sistematici monitoraggi della rete interna (intranet) aziendale al fine di evitare la commissione di reati:
- verificare periodicamente le movimentazioni del sistema, in grado di segnalare comportamenti anomali;
- programmare riunioni periodiche con l'ufficio IT e la società di consulenza esterna ai fini della revisione dei risultati dei monitoraggi delle movimentazioni sul sistema;
- individuare almeno due uffici di installazione dei server centrali a livello nazionale;
- installare server con meccanismi di ridondanza in grado di garantire la funzionalità del sistema in caso di malfunzionamenti di singole componenti;
- dotare il sistema di almeno una doppia protezione firewall, assicurando, però, l'assenza di conflitti;
- garantire un sistema permanente di back up esterno di tutti i dati, fisso e/o con sistema cloud con massimi sistemi di sicurezza per l'accesso da remoto (es. implementazione del sistema cloud con metodologie "Internet Security Gateway");
- disporre di un piano di "disaster recovery";
- inserire dati veritieri ed utilizzare i sistemi di personalizzazione delle password al fine di tracciare l'intervento dei diversi soggetti: solo i soggetti espressamente e previamente identificati ed autorizzati possono procedere all'inserimento di dati nei sistemi di enti pubblici, istituti di credito e organi di controllo;
- modificare periodicamente le password di accesso;
- proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili contro l'accesso abusivo da parte di chiunque si introduca nel sistema informatico o telematico attraverso strumenti hardware o software;
- predisporre una pianificazione degli interventi di formazione finalizzati a:
- rendere edotti gli incaricati del trattamento sui rischi che incombono sui dati;

- rendere edotti gli incaricati del trattamento sulle misure disponibili per prevenire eventi dannosi;
- rendere edotti gli incaricati del trattamento sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- rendere edotti gli incaricati del trattamento sulle responsabilità che ne derivano;
- rendere edotti gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- procedere ad una tempestiva segnalazione all'Organismo di Vigilanza nel caso in cui si ravvisino anomalie o carenze nel rispetto dei principi e delle norme di comportamento sopra esposte.

Inoltre, è fatto divieto di:

- utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo;
- introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza;
- procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione apparecchiature dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento;
- installare illegittimamente o abusivamente apparecchiature atte ad intercettare, impedire, interrompere comunicazioni informatiche o telematiche;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;

- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introduzione o trasmissione di dati, informazioni o programmi al fine distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.
- la società si è dotata dell'adeguamento al GDPR e quindi vi è un documento cui fare riferimento anche perché secondo il GDPR, la disciplina dovrebbe rispettare i seguenti punti: a) definire esaustivamente i ruoli attribuiti ai vari attori coinvolti nella procedura anche dal punto di vista dell'organigramma privacy; b) garantire adeguate misure di sicurezza del dato personale e/o sensibile trattato; c) in caso di multinazionali, disciplinare le modalità di eventuali trasferimenti di dati tra Stati extra-europei; d) disciplinare il diritto di accesso del soggetto segnalato agli atti.

B. "PROCEDURE 231"

Politica anticorruzione e rapporti con clienti

La presente parte costituisce una specificazione del sistema di prevenzione e, in particolare, dei cd. Protocolli, in relazione a specifici settori da considerare come "aree sensibili" e per le quali la Società ritiene di dover procedere ad una maggior precisazione nella regolamentazione.

La presente parte potrà essere ulteriormente implementata in occasione di una di ulteriore proceduralizzazione delle attività e delle funzioni aziendali: le procedure adottate andranno ad integrare l'attuale sistema di "procedure 231".

Si fa presente, sotto questo profilo, che anche i contatti, diretti e indiretti, tra la Società e clienti, fornitori e terze parti costituiscono un'area sensibile con riferimento alla possibilità di commissione di varie tipologie di illeciti previsti dal Decreto.

Il Protocollo qui disciplinato funge da regola generale e da prescrizione vincolante nei rapporti con i predetti soggetti indicando i criteri di comportamento che devono essere scrupolosamente osservati.

Rapporti con clienti, fornitori e terze parti:

 I rapporti sono improntati a criteri di trasparenza e professionalità, in uno spirito di massima collaborazione e nel rispetto dei principi fissati nel Codice Etico.

 Tali rapporti sono intrattenuti dalle varie funzioni aziendali a ciò preposte a seconda dell'importanza e della rilevanza della problematica di volta in volta in rilievo; le varie funzioni aziendali coinvolte redigono relazioni o rapporti scritti sullo stato delle varie pratiche che devono essere archiviati e messi a conoscenza dei responsabili in via gerarchica.

 La redazione dei suddetti rapporti può essere periodica o può avvenire anche a seguito di singoli incontri in relazione all'importanza e allo stato della pratica. In ogni caso, è fatto obbligo di segnalare eventuali situazioni anomale che determinino una variazione nell'iter amministrativo rispetto alle normali prassi. Le relazioni o i rapporti vanno compilati e conservati nell'archivio di ciascuna pratica.

 Quando è in corso qualsiasi trattativa, richiesta o rapporto, il personale incaricato non deve cercare di influenzare impropriamente le decisioni delle controparti che trattano o prendono decisioni, né tanto meno porre in essere, direttamente o indirettamente, azioni quali:

- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare controparti a titolo personale;

- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti al di fuori di quanto consentito dalla legge;

- effettuare attività di mediazione, sfruttando o vantando asseriti o esistenti rapporti ovvero ponendo in essere condotte che violino i principi di trasparenza e onestà di cui al Codice Etico.

 ogni richiesta di contributi, finanziamenti o altre erogazioni concessi o erogati dallo Stato, da altri enti pubblici e dalle Comunità europee deve essere preventivamente autorizzata dall'Amministratore, che ne deve verificare la corrispondenza alle norme di legge;

 ogni flusso di denaro erogato e la provenienza e la destinazione di tali somme devono essere adeguatamente giustificati e devono essere portati a conoscenza dell'Organismo di Vigilanza;

 qualora nei rapporti intercorrenti con le controparti siano necessari degli esborsi da parte della Società, tali operazioni dovranno essere preventivamente sottoposte ad

autorizzazione dell'Amministratore, che ne deve verificare la corrispondenza alle norme di legge e ai regolamenti aziendali;

 chiunque venga a conoscenza di qualsiasi forma di violazione ai presenti precetti, deve prontamente informare l'Organismo di Vigilanza;

Si precisa che i predetti processi costituiscono parte integrante della politica anticorruzione e dei rapporti con i clienti e le terze parti.

B.1. PROCEDURE IN MATERIA DI SICUREZZA

Principi generali

Per le principali attività svolte da Mareca si implica il rispetto di peculiari regole in tema di salute e sicurezza del lavoro.

Mareca dovrà assicurarsi che le imprese fornitrici utilizzate, nonché il proprio personale, siano informati sulle norme di sicurezza nazionali, siano opportunamente formati ai sensi del D.lgs 81/2008 in relazione alle attività e mansioni da svolgere ed eventualmente dotati dei d.p.i. specifici per la mansione, siano a conoscenza dei documenti inerenti la sicurezza e dei rischi di interferenza.

Regole operative

Mareca adotta i regolamenti e le disposizioni in materia di sicurezza emanata dal gestore per ogni singolo evento.

Mareca sulla base della propria articolazione delle funzioni antinfortunistiche, identifica il soggetto responsabile per la gestione degli adempimenti gravanti sulla stessa per effetto dei regolamenti.

Mareca adempie, per quanto di competenza, agli obblighi di formazione e informazione dei propri lavoratori e garantisce lo scambio delle informazioni con gli altri destinatari degli obblighi antinfortunistici al fine di assicurare le migliori azioni prevenzionali nel caso di lavori con rischio da interferenza.

B.2. PROCEDURE DI GESTIONE DELL'UFFICIO ACQUISTI

La definizione della procedura di gestione degli acquisti assume rilievo primario ai fini della effettività del Modello 231/01. Infatti, non solo la gestione proceduralizzata degli approvvigionamenti garantisce maggiore efficienza imprenditoriale ed economica, ma altresì permette di orientare ogni modalità operativa al rispetto della legge e, più in particolare, alla prevenzione di condotte di natura corruttiva e anticoncorrenziale.

Per tale ragione si è ritenuto opportuno inserire la procedura di gestione dell'Ufficio Acquisti direttamente all'interno della Parte Speciale del Modello 231.

La procedura riguarda le B.U. Procurement Office, Logistics Department, Engineering Office, Production Department e Planning Office.

Principi Generali.

Le procedure di acquisto sono orientate alla massima trasparenza, tracciabilità e rintracciabilità dei processi, nel rispetto dei principi di efficacia, non discriminazione economicità, tempestività, correttezza, libera concorrenza, parità di trattamento, pubblicità.

Le procedure di acquisto digitalizzate sono gestite tramite software dedicati che devono essere strutturati secondo i parametri stabiliti in materia dalla compliance normativa nazionale e internazionale.

L'intero processo di acquisto è condotto attraverso un sistema automatizzato in tutte le sue fasi, dalla richiesta di acquisto, alla negoziazione o (quando necessario) gara telematica, fino alla formalizzazione del servizio e relativo ordine, garantendo massima tracciabilità.

La procedura di acquisto deve permettere di:

- selezionare, qualificare e valutare i migliori fornitori
- applicare correttamente gli aspetti legali necessari alla definizione di contratti di acquisto completi
- valutare gli strumenti e le metodologie legate all'ascolto del cliente interno e verificare la congruenza della richiesta di acquisto con i budget disponibile

- classificare, razionalizzare e definire gli obiettivi economici ed operativi legati alle aspettative delle funzioni interne
- confrontare e riflettere sulla propria realtà in relazione al processo di acquisto ideale
- operare la scelta del miglior fornitore secondo procedure trasparenti.

Le fasi di lavoro principali e più critiche riguardano e devono prevedere:

1. la definizione dei fabbisogni, ovvero la necessità di tracciare l'esigenza di un approvvigionamento e raggiungere una corretta identificazione del fabbisogno manifestato da una risorsa aziendale e quindi, in ultima analisi, di compilare una richiesta di offerta conforme al bisogno.

   L'esigenza deve essere formalizzata e deve essere condivisa con tutti i soggetti coinvolti e con i responsabili dei vari livelli autorizzativi;

2. la valutazione, selezione e monitoraggio dei fornitori, ovvero la necessità di tracciare il percorso di selezione di un fornitore, per dare riscontro del percorso valutativo eseguito dai vari soggetti intervenuti in modo del tutto trasparente anche nel confronto di potenziali competitor.

   Deve essere previsto e aggiornato periodicamente un elenco dei fornitori qualificati, almeno per i fornitori ritenuti strategici e critici, di cui venga effettuata la valutazione anche sotto il profilo della *vendor compliance*, nel rispetto dei requisiti di etica, professionalità e competenza. Ciò garantisce di instaurare rapporti con i soli fornitori che, oltre ad offrire la qualità richiesta, possano garantire la non esposizione dell'azienda al rischio di commissione di uno dei reati disciplinati dal D.lgs 231/2001. La tracciabilità del percorso valutativo dei fornitori garantisce anche il rispetto del principio della trasparenza e della *governance*, potendo motivare e documentare la scelta compiuta.

   Deve essere effettuato un costante monitoraggio e valutazione delle performance del parco fornitori nel corso del rapporto contrattuale, prevedendo "clausole 231 e "Decreto 81" che obblighino alla comunicazione da parte del fornitore di tutti i dati legati agli aspetti di responsabilità amministrativa e Salute e Sicurezza sul lavoro (ad esempio: Dichiarazione Idoneità Tecnico

Professionale, Estratto Libro Unico Lavoratori dei soggetti impiegati nell'Appalto);

3. la negoziazione del contratto, ovvero il controllo del percorso di maturazione della trattativa, e dei contributi forniti dai vari soggetti intervenuti, in particolare i fornitori e i decisori lato committente (potendo altresì assicurare che nella conduzione della trattativa siano state evitate situazioni nelle quali i soggetti coinvolti siano o possano apparire in conflitto di interesse).

   La corrispondenza e le informazioni tra i vari soggetti che intervengono nella negoziazione deve essere condivisa con tutti i soggetti coinvolti e con i responsabili dei vari livelli autorizzativi, evitando di lasciare autonomia operativa, autorizzativa e di verifica, in capo a un unico soggetto;

4. la disposizione di ordine, ovvero l'esigenza tracciare l'invio di un ordine al fornitore e regolare per iscritto tutte le forniture di servizi, così da permettere la comparazione tra l'ordine e la fattura emessa dal fornitore.

   A tal fine gli ordini devo essere emessi solo tramite l'utilizzo di un software aziendale tracciabile (che prevede l'inserimento in anagrafica del soggetto, tracciandone la presenza), e devono essere regolate in forma scritta tutte le forniture di servizi: i contratti/mandati devono essere formalizzati e devono indicare chiaramente l'oggetto del servizio richiesto (o dell'incarico professionale conferito), nonché il compenso pattuito;

5. la verifica della prestazione, che deve prevedere il tracciamento della avvenuta erogazione di un servizio o la consegna di un prodotto, in modo da comprovare che il pagamento corrisponde a una esigenza reale, coerente con quanto ordinato. Inoltre, deve essere compilato un modulo di verifica e descrizione delle performance del servizio prodotto offerto dal fornitore, (qualità nella consegna, tempi, disponibilità del fornitore attraverso indicatori sintetici e immediati), affinché sia garantita una corretta verifica tra la qualità richiesta del servizio/prodotto e la qualità effettivamente offerta, attuando le eventuali azioni correttive verso il fornitore.

la verifica che i procedimenti e dei sistemi a supporto del processo di acquisto end-to-end siano allineati ad una compliance normativa nazionale e internazionale che garantisca la negoziazione o la gara telematica, fino alla formalizzazione del servizio e

relativo ordine-fattura. I sistemi di approvvigionamento elettronico aiutano i responsabili degli uffici acquisti in tutte le fasi organizzative

B.2. PROCEDURE SPECIALI

La definizione della procedura di gestione degli acquisti assume rilievo primario ai fini della effettività del Modello 231/01. Infatti, con alcuni clienti (vds. IKEA) si è procedimentalizzata la gestione degli approvvigionamenti al fine di orientare ogni modalità operativa al rispetto della legge e, più in particolare, alla prevenzione di condotte di natura corruttiva e anticoncorrenziale.

Per tale ragione si è ritenuto opportuno inserire la procedura di gestione all'interno della Parte Speciale del Modello 231.

Principi Generali.

Le procedure speciali sono orientate alla massima trasparenza, tracciabilità e rintracciabilità dei processi, nel rispetto dei principi di efficacia, non discriminazione economicità, tempestività, correttezza, libera concorrenza, parità di trattamento, pubblicità.

Le procedure di acquisto digitalizzate sono gestite tramite regole dedicate coem ad esempio IWAY che devono essere strutturati secondo i parametri stabiliti al gfine del rispetto della compliance richiesta.

L'intero processo è condotto attraverso un sistema automatizzato in tutte le sue fasi, dalla richiesta di acquisto, alla negoziazione o (quando necessario) gara telematica, fino alla formalizzazione del servizio e relativo ordine, garantendo massima tracciabilità ed assoluta mappatura.

La procedura deve permettere di:

- applicare correttamente gli aspetti legali necessari alla definizione dei contratti e valutare gli strumenti e le metodologie legate al rapporto con il cliente
- classificare, razionalizzare e definire gli obiettivi economici ed operativi legati alle aspettative delle funzioni interne

- confrontare e riflettere sulla propria realtà in relazione al processo di acquisto ideale
- operare la scelta del miglior fornitore secondo procedure trasparenti.

Le fasi di lavoro principali devono prevedere:

6. la definizione del rapporto con il cliente con un alto standard di servizio. L'esigenza deve essere formalizzata e deve essere condivisa con tutti i soggetti coinvolti e con i responsabili dei vari livelli autorizzativi
7. la valutazione, selezione e monitoraggio e la necessità di tracciare il percorso di selezione, per dare riscontro del percorso valutativo eseguito dai vari soggetti intervenuti in modo del tutto trasparente anche nel confronto di potenziali competitor.

Viene richiesta la corrispondenza e le informazioni tra i vari soggetti che intervengono nella negoziazione deve essere condivisa con tutti i soggetti coinvolti e con i responsabili dei vari livelli autorizzativi, evitando di lasciare autonomia operativa, autorizzativa e di verifica, in capo a un unico soggetto;

A tal fine gli ordini devo essere emessi solo tramite l'utilizzo di un software aziendale tracciabile (che prevede l'inserimento in anagrafica del soggetto, tracciandone la presenza), e devono essere regolate in forma scritta tutte le forniture di servizi: i contratti/mandati devono essere formalizzati e devono indicare chiaramente l'oggetto del servizio richiesto (o dell'incarico professionale conferito), nonché il compenso pattuito;

La verifica che i procedimenti e dei sistemi a supporto del processo di acquisto end-to-end siano allineati ad una compliance normativa nazionale e internazionale che garantisca la negoziazione o la gara telematica, fino alla formalizzazione del servizio e relativo ordine-fattura. I sistemi di approvvigionamento elettronico aiutano i responsabili degli uffici acquisti in tutte le fasi organizzative

SCHEDA SINTETICA DEI CD. REATI PRESUPPOSTO E DELLE PRINCIPALI MODALITÀ DI COMMISSIONE DEGLI STESSI CON RIFERIMENTO AGLI ILLECITI 231INDIVIDUATI, ALL'ESITO DELL'AGGIORNAMENTO DELLA MAPPATURA, QUALI "REATI 231 A RISCHIO RILEVANTE DI COMMISSIONE"[1]

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.

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

La frode informatica, invece, assume rilievo ai fini della responsabilità dell'ente solo se realizzata in danno della P.A. Il reato di frode informatica presenta, sostanzialmente, la medesima struttura e i medesimi elementi costitutivi del reato di truffa da cui si distingue in quanto l'attività illecita investe non la persona ma un sistema informatico. Nel reato di frode informatica, pertanto, non assume rilevanza - a differenza che nel reato di truffa - il ricorso da parte dell'autore del reato ad artifizi o raggiri, ma l'elemento oggettivo dell'alterazione del sistema informatico (e/o dei dati in esso disponibili).

Le fattispecie di cui agli artt. art. 316 bis, 316 ter e 640 bis c.p. 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.

Aree a rischio reato	Controlli preventivi
Partecipazione ad una gara indetta da un soggetto pubblico, ovvero	➔ specifiche previsioni nel sistema aziendale di programmazione e di

[1] Tratte da "*DECRETO 231. LE NUOVE LINEE GUIDA DI CONFINDUSTRIA PER LA COSTRUZIONE DEI MODELLI ORGANIZZATIVI",* aggiornate al marzo 2014.

presentazione di istanze alla P.A. al fine di ottenere il rilascio di un atto o di provvedimento amministrativo di interesse (ad es. mediante la produzione di documenti falsi attestanti l'esistenza di condizioni e/o requisiti essenziali).	controllo; ➔ puntuali attività di controllo gerarchico (incluso sistema di deleghe);
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; ✓ i rapporti con soggetti della P.A. competenti in materia fiscale o previdenziale in relazione alla ipotesi di modifica in via informatica dei dati (es. fiscali e/o previdenziali) di interesse dell'azienda (es. modelli 770), già trasmessi alla P.A.	➔ sistema di controlli interno all'azienda 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 aziendali; ✓ la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dalla società; ✓ il rispetto della normativa sulla privacy.
Le aree maggiormente a rischio riguardano: ✓ settore delle attività finanziarie in particolare in relazione alla gestione di finanziamenti pubblici; ✓ area organizzativa incaricata della gestione delle sponsorizzazioni e dei fondi ottenuti tramite pubbliche contribuzioni anche per manifestazioni all'estero; ✓ investimenti per formazione.	➔ programma di informazione e/o 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'azienda 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 delle funzioni 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: ✓ settore delle attività finanziarie in particolare in relazione alla gestione di finanziamenti pubblici; ✓ area organizzativa incaricata della gestione delle sponsorizzazioni e dei fondi ottenuti tramite pubbliche contribuzioni anche per manifestazioni all'estero; ✓ investimenti per formazione.	➔ controlli di completezza e correttezza della documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto); ➔ 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

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

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

Quanto ai soggetti maggiormente esposti a tale fattispecie di reato si fa riferimento a coloro che utilizzano in maniera rilevante gli strumenti informatici e telematici per lo svolgimento delle proprie attività: tale categoria di reato risulta di più probabile accadimento in quei settori attivi nella gestione 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 R&S, area ICT, area acquisti e appalti) che risultano maggiormente esposte al rischio di commissione di reati informatici che possano determinare un interesse o un vantaggio economico per l'ente.

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;
- ➔ 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 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;
- ➔ previsione di idonee clausole nei contratti conclusi con i provider di servizi legati all'Information Technology.

A ciò si aggiunga la necessità l'adozione si policy e procedure organizzative concernenti:

- ➔ l'utilizzo di apparecchi personali sul luogo di lavoro (cd. BYOD policy), qualora ammessi, che prevedano, a titolo esemplificativo: i) la regolamentazione dell'uso dei suddetti apparecchi (quali tablet e smartphone) a fini lavorativi; ii) la selezione e definizione di browser, programmi, social network e applicazioni il cui uso è permesso/tollerato/limitato/vietato all'interno del contesto aziendale; iii) l'adozione di sistemi di logging e di monitoring nei limiti consentiti; iv) la previsione di un sistema interno di gestione degli apparecchi, comprendente la programmazione degli stessi e l'assistenza tecnica; v) l'adozione di azioni di cancellazione di dati e bloccaggio in remoti dei dispositivi;
- ➔ l'utilizzo di sistemi di cd. cloud computing che prevedano, a titolo esemplificativo: i) la scelta dei cd. cloud server ammessi sulla base di criteri stabiliti da policy interne (es. affidabilità del gestore, accessibilità del servizio, ecc.); ii) la regolamentazione e/o restrizione dell'uso di servizi di clouding per il salvataggio e la trasmissione di determinate tipologie di documenti aziendali; iii) la definizione e diffusione di linee guida per l'utilizzo dei servizi di clouding da parte di tutti gli esponenti dell'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.

E' auspicabile l'adozione di un sistema ICT Security Governance & Management e comunque di un sistema in grado di assicurare 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. 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, ecc.).

Modalità di realizzazione del reato	Controlli preventivi[2]
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). 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). 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).
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	➔ 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

[2] Le specifiche misure di controllo preventivo indicate in tabella sono riprese dallo standard ISO 27001:2005, di cui in parentesi è riportata la numerazione

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 geografiche di riferimento, 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.	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 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 che competono al ruolo 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 (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).
<u>Art. 615-quater c.p.</u> 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 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	➔ 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).

l'ente.	
<u>Art. 617-quater e 617-quinquies c.p.</u> Intercettazione fraudolenta di comunicazioni di enti concorrenti nella partecipazione a gare di appalto o di fornitura svolte su base elettronica (e-market place) 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	➔ 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 dalla 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: (i) rete e informazioni che vi transitano (A.10.6.1); (ii) instradamento (routing) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza (A.11.4.7); (iii) 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).
<u>Art. 615-quinquies, 635 bis, 635 quater c.p.</u> Danneggiamento di informazioni, dati e programmi 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. Danneggiamento di informazioni, dati,	➔ 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);

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.	➔ 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).
<u>Art. 635-ter, 635 quinquies c.p.</u> 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	➔ predisposizione di misure volte alla protezione dei documenti elettronici (es. firma digitale); ➔ elaborazione di procedure per

per il rilascio di certificati qualificati (es. identificabilità univoca del titolare, titolarità certificata), con lo scopo di mantenere un alto numero di certificati attivi. Aggiramento dei vincoli imposti dal sistema per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre così un guadagno all'ente.	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.

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.

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

A tale proposito si deve ricordare che, secondo l'attuale disciplina, ciò che rileva è, infatti, l'attività svolta in concreto e non la natura giuridica, pubblica o privata, del soggetto. Ne consegue che il nostro ordinamento accoglie una nozione di pubblico ufficiale e di incaricato di pubblico servizio di tipo "oggettivo", che comporta la necessità di una valutazione "caso per caso" 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.

Ai fini della gestione del modello organizzativo, è importante distinguere le fattispecie in esame e considerarne le differenti caratteristiche strutturali che possono essere così sintetizzate:

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.

Ai fini dell'aggiornamento del Modello l'introduzione ex novo del delitto di induzione indebita a dare o promettere utilità, può comportare, ferma restando la specificità di ogni singolo contesto, 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 di potenziale esposizione al rischio tenderanno a comprendere tutti gli ambiti di operatività contraddistinti da rapporti con soggetti pubblici (oltre che le attività eventualmente svolte da parte di un esponente dell'azienda in qualità di pubblico ufficiale o di incaricato di pubblico servizio in veste, in tal caso, di colui che "induce" alla prestazione indebita), con un ampliamento delle aree interessate dal 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.

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

altri un indebito vantaggio in operazioni economiche internazionali o per mantenere una attività economica o finanziaria.

Premesso quanto sopra, si rinvia alla tabella seguente per l'identificazione, in via meramente esemplificativa, le principali macro aree da considerarsi direttamente a rischio reato, con l'evidenziazione di alcuni possibili presidi e controlli preventivi da implementare nel contesto aziendale, nell'ambito di un organico sistema procedurale, ai fini della loro copertura.

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.

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: (i) Autorità Indipendenti e di Vigilanza e altri organismi di diritto pubblico; (ii) pubblici ufficiali e incaricati di pubblico servizio relativamente agli adempimenti fiscali, tributari e previdenziali (iii) 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	➔ 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; ➔ procedure di tracciabilità dei flussi finanziari aziendali con l'individuazione dei soggetti autorizzati all'accesso alle risorse; ➔ verifiche, a cura di idonee funzioni distinte da quella "commerciale", sull'effettiva erogazione delle forniture e/o sulla reale prestazione dei servizi, inclusi i controlli sui livelli qualitativi attesi, anche ai fini della risoluzione di possibili contestazioni del cliente a fronte di ipotesi di disservizi; ➔ presidi specifici a fronte del ricorso a partnership commerciali, intermediazioni e forme aggregative tra enti quali, ad es. ricorso ad attestazioni in ottica 231, attivazione sistemi di monitoraggio gestionale estesi alle aree di interesse, etc.; ➔ controlli dei collaboratori esterni (ad esempio agenti e intermediari) e della congruità delle provvigioni pagate rispetto a quelle praticate nell'area geografica di riferimento; ➔ monitoraggio dei procedimenti 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 finanziarie e di strumenti finanziari derivati. 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.	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;	➔ predisposizione di specifiche procedure organizzative relative ad acquisti, consulenze, sponsorizzazioni, reclutamento del personale, spese di rappresentanza, gestione della finanza, ecc.), assicurando per esempio: ✓ verifiche preventive sulle controparti o sui beneficiari; ✓ definizione di criteri qualitativi e 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 gara o di negoziazione diretta, indette da organismi pubblici dell'Unione Europea o stranieri o a similari procedure svolte in un contesto competitivo a carattere internazionale.	➔ procedimentalizzazione dei rapporti e delle operazioni che si svolgono nelle aree geografiche a maggiore rischio reato, eventualmente adottando particolari cautele già nella fase precontrattuale e di negoziazione, nonché nella individuazione dei soggetti incaricati delle relative operazioni e nello scambio di comunicazioni formali che ne attestino la trasparenza e correttezza; ➔ consultazione di studi e rilievi analitici, ormai consolidati e di particolare attendibilità, che periodicamente enti specializzati svolgono per valutare il

	livello di corruzione nelle pubbliche amministrazioni in tutti i paesi del mondo.
Partecipazione a procedure di evidenza pubblica in associazione con altri partner (RTI, ATI, joint venture, consorzi, etc.).	➔ verifiche preventive sui potenziali partner; ➔ 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; ➔ eventuale definizione di specifiche clausole contrattuali di audit 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-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. 2635 bis Istigazione alla 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*

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*".

I reati societari possono qualificarsi come propri perché soggetti attivi possono essere solo "amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza".

Modalità di realizzazione del reato attività a rischio reato	**Controlli preventivi**
<u>False comunicazioni sociali</u>. Redazione del bilancio, delle relazioni o elle 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	➔ previsione nel Codice etico di norme riguardanti il corretto comportamento di tutti i dipendenti coinvolti nelle attività di formazione del bilancio o di altri documenti similari, così da garantire: (i) massima collaborazione; (ii) completezza e chiarezza delle informazioni fornite; (iii) accuratezza dei dati e delle elaborazioni; (iv) 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.); ➔ stituzione 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. ➔ se il bilancio è assoggettato a revisione e certificazione, è consigliabile a) elaborare a cura dell'Amministratore per l'approvazione dello stesso: la bozza del bilancio, allegando una documentata certificazione dell'avvenuta consegna della bozza in questione; la lettera di attestazione o di manleva richiesta dalla società di revisione, ove esistente, sottoscritta dal massimo vertice esecutivo e siglata dal Responsabile amministrativo; b) prevedere almeno una riunione tra la società di certificazione, il Collegio Sindacale, il Comitato per il controllo e rischi (ove esistente) e l'Organismo di Vigilanza, per il bilancio, che abbia per oggetto tale documento, da documentarsi mediante verbale; comunicare sistematicamente all'Organismo di Vigilanza gli incarichi conferiti, o che si intende conferire, alla società di revisione (se esistente) o a società ad essa collegate, diverso da quello concernente la certificazione del bilancio; valutazioni in ordine alla scelta della società di revisione (in base ad elementi quali professionalità, esperienza nel settore non solo in base all'economicità);

	➔ per gli enti il cui bilancio non è assoggettato a revisione e certificazione, si suggerisce di prevedere: (i) 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; (ii) almeno un incontro all'anno, in prossimità della riunione dell'Amministratore, tra Organismo di Vigilanza e Collegio sindacale avente per oggetto il bilancio (con relativa nota integrativa), con redazione di verbale.
<u>Impedito controllo</u>. Gli amministratori di una società a fronte di una puntuale richiesta da parte del Collegio Sindacale in ordine al rispetto, da parte della società, di una determinata normativa, tengono una condotta non corretta e trasparente. In particolare, non assecondano la richiesta di informazioni da parte del Collegio sindacale mediante l'occultamento, anche accompagnato da artifici, della documentazione utile a rappresentare i processi applicativi in sede aziendale di tale legge oppure l'esibizione parziale o alterata di detta documentazione. Perché tale condotta costituisca illecito ai sensi del decreto 231 deve derivare da essa un danno per la società.	➔ esistenza di un sistema definito di responsabilità del vertice aziendale e di deleghe coerenti; ➔ istituzione di riunioni periodiche tra Collegio Sindacale, Comitato di controllo e rischi (se esistente) ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/Corporate Governance, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del management e dei dipendenti; ➔ riporto periodico al Vertice sullo stato dei rapporti con il Collegio Sindacale e le altre Autorità abilitate ai controlli sulla Società.
<u>Illecita influenza sull'assemblea</u>. L'Amministratore 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)	➔ istituzione di riunioni periodiche tra Collegio Sindacale ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del management, dei dipendenti.

che il reato non si verifica allorché - anche in assenza di una condotta illecita dell'Amministratore - la maggioranza sarebbe stata ugualmente raggiunta.	
<u>Illecite operazioni sulle azioni o quote sociali o della società controllante</u>. L'amministratore dà a un terzo l'incarico di acquistare e/o sottoscrivere azioni in nome proprio e per conto della società. <u>Operazioni in pregiudizio dei creditori</u>. 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	➔ programma di informazione/formazione periodica degli amministratori, del management e dei dipendenti sulla normativa di Corporate Governance e sui reati/illeciti amministrativi in materia societaria; ➔ 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; ➔ procedure di (i) autorizzazione dell'acquisto di azioni o quote proprie e/o della società controllante; (ii) di disciplina delle operazioni di riduzione del capitale sociale, fusione e scissione societaria.
<u>Corruzione tra privati</u>. Costituiscono aree a rischio reato: ✓ la predisposizione di bandi di gara/partecipazione a procedure competitive finalizzati alla negoziazione o stipula di contratti attivi, cioè in grado di generare un ricavo per la società; ✓ la negoziazione, stipula e gestione di contratti attivi con società, consorzi, fondazioni associazioni e altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa; ✓ la 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	➔ 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: ✓ 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

rating, organismi di certificazione e di valutazione di conformità, etc.); ✓ la selezione dei fornitori di beni e servizi, negoziazione e stipula dei relativi contratti; ✓ la 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 (o al Direttore Generale se nominato) 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 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.	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. ➔ nei rapporti con società, consorzi, fondazioni, associazioni ed altri enti privati, devono essere adottati e attuati uno o più strumenti normativi e/o organizzativi che nell'ambito dei rapporti con società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgano attività professionali/istituzionali o di impresa dal cui svolgimento o mancato svolgimento possa derivare un vantaggio per la società o per le quali la stessa possa avere un interesse prevedano: ✓ l'individuazione delle tipologie di rapporti e le relative modalità di gestione; ✓ le modalità di raccolta, verifica e approvazione della documentazione da trasmettere agli esponenti di società, consorzi, fondazioni, associazioni ed altri enti privati, anche privi di personalità giuridica, che svolgano

	attività professionale e di impresa per le quali l'ente abbia un interesse o dalle quali possa derivare un vantaggio, con il supporto delle funzioni competenti. ➔ inserimento nel Codice etico di specifiche previsioni riguardanti il corretto comportamento di tutti i dipendenti coinvolti in rapporti con società concorrenti o target (ad. es., rispetto delle regole di corretta concorrenza; trasparenza e tracciabilità dei comportamenti; divieto di regalie o promesse di benefici).; ➔ attività di formazione di base verso tutti i responsabili di funzione, particolarmente dell'area commerciale, ricerca e sviluppo, progetti speciali e dell'alta dirigenza, affinché conoscano le principali nozioni in tema di reato di corruzione privata (in particolare norme di legge, sanzioni, fattispecie a rischio reato). ➔ adozione di regole comportamentali da seguire nella gestione di rapporti con professionisti e soggetti appartenenti a società terze, che prevedano: ✓ 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.
Approvvigionamento di beni, lavori e servizi	➔ adozione di procedure di autorizzazione delle richieste di acquisto che prevedano: ✓ criteri e 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. limitati e chiaramente individuati

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 o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro**; Codice penale art. 590* ***Lesioni personali colpose

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, nonché con l'esimente di cui all'art. 6, nella parte in cui richiede la prova della elusione fraudolenta del modello organizzativo, sicuramente incompatibile con una condotta colposa. A tal proposito, l'impasse si potrebbe superare facendo ricorso ad una interpretazione che, tenendo conto del diritto di difesa e del principio di uguaglianza, permetta di prescindere da tale prova o quantomeno di disancorare il concetto di "elusione fraudolenta" dalle tipiche fattispecie proprie del codice penale e di assumerlo in termini di intenzionalità della sola condotta dell'autore (e non anche dell'evento) in violazione delle procedure e delle disposizioni interne predisposte e puntualmente implementate dall'azienda per prevenire la commissione degli illeciti di cui si tratta o anche soltanto di condotte a tali effetti "pericolose". Questa interpretazione si fonda sui seguenti presupposti. Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche. In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare le 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.
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. Quest'ultimo, per essere efficacemente attuato, potrà utilmente essere

integrato con il "sistema" degli adempimenti aziendali nascenti dagli obblighi di prevenzione e protezione imposti dall'ordinamento legislativo (v. sopra) e, qualora presenti, con le procedure interne nascenti dalle esigenze di gestione della sicurezza sul lavoro. Da qui l'opportunità che l'azienda ponga in essere azioni mirate volte garantire la suddetta integrazione (anche in vista della successiva eventuale verifica da parte del Giudice) ed in particolare: • effettuazione di una mappatura del rischio approfondita e orientata secondo le specificità dell'attività produttiva presa in considerazione; • attenta verifica ed eventuale integrazione delle procedure interne di prevenzione ai sensi del decreto 231 in coerenza con la specificità dei rischi di violazione delle norme richiamate dall'art. 25-septies; a tal fine sarà importante tenere conto e armonizzare tutte le attività già svolte, anche in materia di gestione della sicurezza, evitando inutili quanto costose duplicazioni; • valutazione ed individuazione dei raccordi tra i vari soggetti coinvolti nel sistema di controllo ai sensi del decreto 231 e delle normative speciali in materia di sicurezza e salute sui luoghi di lavoro, con particolare riferimento alla previsione di un sistema integrato di controllo riguardante il Responsabile dei servizi di prevenzione e protezione (RSPP o altro soggetto giuridicamente equivalente) qualificabile come controllo tecnico-operativo o di primo grado, e l'Organismo di Vigilanza.

SCHEDA SINTETICA DEGLI ULTERIORI REATI PRESUPPOSTO INDIVIDUATI, ALL'ESITO DELL'AGGIORNAMENTO DELLA MAPPATURA, QUALI "REATI 231 A RISCHIO NON RILEVANTE DI COMMISSIONE"

"Reati 231 a rischio non rilevabile di commissione

(3) Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001)

(5) Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D.Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs. 125/2016]

(8) Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D.Lgs. n. 231/2001)

(9) Pratiche di mutilazione degli organi genitali femminili (Art. 583-bis c.p.) (Art. 25-quater.1, D.Lgs. n. 231/2001)

(10) Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001)

(11) Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001)

(15) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001)

(16) Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001

(17) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.Lgs. n. 231/2001)

(18) Delitti di razzismo e xenofobia (Art. 25-terdecies, D.Lgs. n. 231/2001)

(19) Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva]

(20) Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

(21) Reati di cui al D.lgs. N. 196/2003 come modificato dal R.E. 679/2016 e dal D.lgs. 101/2018

(22) Corruzione tra privati (art. 25-ter, lett. s-bis) ed induzione indebita a dare o promettere utilità (art. 25).

(23) Art. 25-octies.1 Delitti in materia di strumenti di pagamento diversi dai contanti

(24) Art. 25-decies. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

(25) Art. 25-duodecies. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

(26) Art. 25-terdecies. Razzismo e xenofobia

(27) Art. 25-quaterdecies. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati

(28) Art. 25-quinquiesdecies. Reati tributari

(29) Art. 25-sexiesdecies. Contrabbando

(30) Art. 25 -septiesdecies. Disposizioni in materia di reati contro il patrimonio culturale [Articolo aggiunto da L.n.22 del 09 Marzo 2022]

(31) Art. 25 – duodevicies. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici [Articolo aggiunto da L.n.22 del 09 Marzo 2022]

(32) Art. 26 – Delitti tentati. (Art.56 c.p.).