MODELLO ORGANIZZATIVO D. LGS. 231/2001

PARTE SPECIALE

TAO GROUP S.R.L.
Via G. di Vittorio 216-218
53042 Chianciano Terme (SI)
C.F./P.IVA 01469200529

Il presente Modello di organizzazione gestione e controllo, ai sensi del d. lgs. 231/2001 è approvato dal C.d.A. il 07.01.2023 e adottato il 09.01.2023

SOMMARIO

SEZIONE 8	**LE FATTISPECIE DI REATI TRIBUTARI.**
8.1.	**DELITTI IN MATERIA DI DICHIARAZIONE.**
8.2.	**DELITTI IN MATERIA DI DOCUMENTI E PAGAMENTO DI IMPOSTE.**
8.3.	**IL SISTEMA DEI CONTROLLI.**
8.4.	**PRINCIPI GENERALI DI COMPORTAMENTO.**

1) ANALISI DEL RISCHIO NELL'ENTE TAO GROUP S.R.L.

Il Decreto legislativo n. 231/2001 individua le fattispecie di reato che, se commesse da soggetti che rivestono una posizione apicale all'interno dell'azienda o da persone sottoposte a direzione o vigilanza degli stessi (cfr. artt. 6-7), costituiscono fonte di responsabilità per gli enti, qualora siano commessi a vantaggio o nell'interesse degli stessi.
L'analisi è stata condotta, a titolo esemplificativo e non esaustivo, attraverso l'esame:

- dell'attività svolta dall'ente;
- della struttura organizzativa;
- della delega di poteri;
- dei contratti che l'ente, in ragione della propria attività stipula con i terzi (collaboratori, fornitori, docenti);
- delle procedure e dei sistemi di controllo interni aggiornati anche in relazione alle certificazioni di qualità ottenute e mantenute.

1.1. CLASSIFICAZIONE DEI REATI.

Proprio in considerazione della natura delle attività svolte dalla Tao Group S.r.l. sono stati **valutati come rilevanti** (in quanto ritenuti potenzialmente a rischio di essere commessi a vantaggio e/o nell'interesse della società), **i reati richiamati dagli articoli**:
artt. 24 e 25 del D. Lgs. 231/2001 (delitti contro la Pubblica Amministrazione), **art. 24 bis** del D. Lgs. 231/2001 (delitti informatici e trattamento illecito di dati), **art. 25 bis** del D.Lgs. 231/2001 (delitti contro la fede pubblica)**, art. 25 bis 1** del D. Lgs. 231/2001 (delitti contro l'industria e il commercio), **art. 25 ter** del D. Lgs. 231/2001 (reati societari), **art. 25 septies** del D. Lgs. 231/2001 (reati di omicidio colposo e lesioni colpose gravi e gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro), **art. 25 octies** del D. Lgs. 231/2001 (ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita), **art. 25 nonies** del D. Lgs. 231/2001 (reati in materia di violazione del diritto d'autore), **art. 25 quindicies** del D. Lgs. 231/2001 (reati tributari).

Alla luce delle valutazioni svolte e dell'analisi condotta **risulta esclusa** la rilevanza dei reati richiamati dagli artt. **artt. 24 ter** del D. Lgs. 231/2001 (delitti di criminalità organizzata);

art. 25 quater del D. Lgs. 231/2001 (delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali), **art. 25 quater 1** del D. Lgs. 231/2001 (pratiche di mutilazione degli organi genitali femminili), **art. 25 quinquies** del D. Lgs. 231/2001 (delitti contro la personalità individuale), **art. 25 sexies** del D. Lgs. 231/2001 (abusi di mercato), **art. 25 octies 1** del D. Lgs. 231/2001 (delitti in materia di strumenti di pagamento diversi dai contanti), **art. 25 decies** del D. Lgs. 231/2001 (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria), **art. 25 undicies** del D. Lgs. 231/2001 (reati ambientali), **art. 25 duodecies** del D. Lgs. 231/2001 (impiego di cittadini di paesi terzi il cui soggiorno è irregolare), **art. 25 terdecies** del D. Lgs. 231/2001 (razzismo e xenofobia), **art. 25 quaterdecies** del D. Lgs. 231/2001 (frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati), **art. 25 sexiesdecies** del D. Lgs. 231/2001 (contrabbando), **art. 25 septesdecies** del D. Lgs. 231/2001 (delitti contro il patrimonio culturale), **art. 25 duodevicies** del D. Lgs. 231/2001 (riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici).

^ ^ ^ ^ ^ ^

Si è ritenuto, infatti, che il rischio di compimento di tali reati da parte di un soggetto che opera nella società o per la società, nello svolgimento di una delle attività dello stesso, rappresenti anche astrattamente un'ipotesi difficilmente configurabile. Pertanto, in riferimento alle predette ipotesi di reato, non configurando attività a rischio, si ritiene sufficiente il richiamo ai principi contenuti nel Codice Etico adottato dalla società e allegato al presente Modello.

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo viene suddivisa a seconda delle diverse tipologie di reati individuate e delle relative misure di controllo, con l'indicazione delle "aree sensibili" emerse dall'analisi delle attività della società che hanno consentito di individuare i rischi/reato sopra indicati.

1.2. SPECIFICHE CIRCA IL DELITTO TENTATO.

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra soceità e soggetti che assumono di agire in suo nome e per suo conto. Si tratta di un'ipotesi particolare del c.d. "recesso attivo", previsto dall'art. 56, comma 4, c.p.

2) LE SINGOLE FATTISPECIE DI REATO EMERSE ALL'ESITO DELL'ANALISI DEL RISCHIO.

SEZIONE 1 - LE FATTISPECIE DI REATO NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ART. 24 E 25 DEL D. LGS. 231/2001).

La conoscenza delle diverse ipotesi di reato e delle modalità di configurazione/consumazione delle stesse, così come circoscritte dal D. Lgs. 231/2001, è presupposto necessario e fondamentale per garantire un sistema di controlli interni funzionale ed efficace alla prevenzione dei reati commessi da "soggetti qualificati" (ex art. 5 del decreto) ed evitare la responsabilità della società.

Agli effetti della legge penale rientra nell'ambito della Pubblica Amministrazione qualsiasi soggetto che:

- svolge attività legislativa, amministrativa o giurisdizionale disciplinata da norme di diritto pubblico;
- persegua, gestisca, realizzi interessi che, per la loro portata, sono ritenuti di pubblico interesse.

A titolo esemplificativo e in relazione alle attività svolte dall'Ente si annoverano tra i soggetti appartenenti alla Pubblica Amministrazione:

- lo Stato, le Regioni, le Province, i Comuni;
- i Ministeri, i Dipartimenti, le Commissioni;
- gli Enti Pubblici non economici (INPS, INAIL, ISTAT..);
- l'Autorità Giudiziaria.

Tra le fattispecie penali qui considerate, il reato di concussione nonché il reato di corruzione, nelle sue varie tipologie, presuppongono il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p. ai sensi dell'art. 357 c.p.:

"1. Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa.

2. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi."

Invece, in base all'art. 358 c.p.:

"1. Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.
2. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale."
In forza delle norme sopra menzionate è possibile attribuire la qualifica di Pubblico Ufficiale a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. In genere, l'esercizio di una pubblica funzione amministrativa viene riconosciuto con riferimento ai soggetti che formano o concorrono a formare la volontà dell'Ente pubblico, che lo rappresentano di fronte ai terzi o che sono muniti di poteri certificativi.
La qualifica di Incaricato di Pubblico Servizio è ravvisabile per esclusione, spettando ai soggetti che svolgono attività di pubblico interesse, alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale e che non consistono in semplici mansioni d'ordine o opere meramente materiali.
In ogni caso, non è necessariamente richiesta la sussistenza di un rapporto di impiego con un Ente Pubblico ai fini del riconoscimento in capo ad un determinato soggetto della qualifica di Pubblico Ufficiale o Incaricato di Pubblico Servizio.
Si illustrano sinteticamente qui di seguito le fattispecie delittuose previste dal decreto.

- **Articolo 316 bis c.p. - Malversazione a danno dello Stato.**

Ipotesi di reato che si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato o da altro Ente Pubblico o dalla Comunità Europea, non si utilizzino le somme ottenute conformemente agli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che si rilevi che l'attività programmata si sia comunque svolta).
Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che solo successivamente vengano destinati a finalità diverse da quelle per cui erano stati erogati.

- **Articolo 316 ter c.p. - Indebita percezione di erogazioni a danno dello Stato.**

Ipotesi di reato che si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità Europea.

In questo caso, a differenza di quanto visto al punto precedente in tema di malversazione, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Inoltre, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa in danno dei medesimi soggetti, nel senso che la punibilità a questo titolo è configurabile solo nei casi in cui non lo sia a titolo di truffa.

- **Articolo 640, comma 2, n. 1 c.p. - Truffa.**

Il reato in questione si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).

- **Articolo 640 bis c.p. - Truffa aggravata per il conseguimento di erogazioni pubbliche.**

Oggetto della truffa in questo caso è l'indebito conseguimento di erogazioni pubbliche.
Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- **Articolo 640 ter c.p. - Frode informatica.**

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato, all'Unione Europea o ad altro Ente Pubblico.
Il reato può essere integrato, ad esempio, qualora, una volta ottenuto un certo finanziamento, venisse violato il sistema informatico al fine di inserire un importo superiore rispetto a quello effettivamente ottenuto legittimamente.

- **Articolo 317 c.p. - Concussione.**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa o induca taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. È ipotizzabile il concorso del privato nella concussione del pubblico ufficiale o dell'incaricato di un pubblico servizio in danno di un altro soggetto privato.

- **Articoli 318 - 319 - 320 c.p. - Corruzione per un atto d'ufficio o per un atto contrario ai doveri d'ufficio.**

Tali ipotesi di reato si configurano nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio ricevano, per sé o per altri, denaro o altri vantaggi per compiere atti contrari al proprio ufficio, ovvero per compiere, omettere o ritardare atti del proprio ufficio (determinando un vantaggio in favore del corruttore). Si ricorda che il reato di corruzione è un reato a concorso necessario, in cui vengono puniti sia il corrotto che il corruttore (cfr. art. 321 c.p.).
Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato è mero soggetto passivo, che subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

- **Art. 319 quater c.p. - Induzione indebita a dare o promettere utilità.**

Punisce accanto al soggetto pubblico, il soggetto privato che, indotto dal pubblico ufficiale o dall'incaricato di un pubblico servizio che abusa del proprio potere, dà o promette denaro o altra utilità al pubblico ufficiale o ad un terzo.

- **Articolo 322 c.p. - Istigazione alla corruzione.**

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli.

1.1. ATTIVITA' SENSIBILI IN RELAZIONE AI REATI CONTRO LA PA.

Le attività potenzialmente "sensibili" riferite ai rapporti con la Pubblica Amministrazione sono qui di seguito elencate:
1) Negoziazione, stipulazione ed esecuzione di contratti con soggetti pubblici: si tratta dell'attività dell'Ente che decide di partecipare, o negoziare/stipulare/eseguire contratti/convenzioni di concessione con la Pubblica Amministrazione mediante procedure negoziate (affidamento o trattativa privata);
2) Gestione Rapporti con enti previdenziali e assistenziali (in particolare INPS, INPDAP e INAIL) con adempimento di quanto previsto dalla relativa disciplina e/o gestione dei relativi accertamenti/ispezioni;
3) Gestione dei rapporti con i soggetti pubblici, relativi all'assunzione di personale anche appartenente a categorie protette o la cui assunzione sia agevolata;
4) Gestione dei rapporti con soggetti pubblici per gli aspetti che riguardano la sicurezza sul lavoro e il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni: si tratta dell'attività connessa agli adempimenti previsti dalla

normativa in materia di sicurezza e igiene sul lavoro e ai relativi rapporti con le Autorità preposte al controllo, anche in caso di ispezioni. (D. Lgs. N. 81/2008);
5) Gestione dei contenziosi giudiziali e stragiudiziali: si fa riferimento ai contenziosi sorti in seguito a cause avviate da e contro l'Ente nei confronti di diversi soggetti (es. soggetti pubblici, dipendenti, clienti e fornitori);
6) Gestione di adempimenti, verifiche, ispezioni a fronte della produzione di rifiuti solidi, liquidi o gassosi, ovvero l'emissione di fumi o la produzione di inquinamento acustico/elettromagnetico soggetti a controlli da parte di soggetti pubblici: si tratta delle attività di gestione degli adempimenti in materia ambientale, tra cui ha particolare rilievo l'adempimento alla normativa sullo smaltimento dei rifiuti. Rientrano nel processo anche i rapporti con soggetti pubblici in occasione di ispezioni da parte di organi di controllo ambientali;
7) Rapporti con Organismi di vigilanza relativi all'adempimento degli obblighi legislativi in materia di privacy: si tratta degli adempimenti e delle prescrizioni previste dalla legge in materia di trattamento della privacy e tutela dei dati personali e della relativa disciplina sanzionatoria (compresa l'applicazione della normativa all'infrastruttura dei sistemi informativi);
8) Gestione dei rapporti con soggetti pubblici per l'acquisizione di finanziamenti/contributi: si tratta dell'attività di richiesta e gestione di contributi/finanziamenti concessi da soggetti pubblici per la realizzazione di attività/servizi, dalla ricerca e individuazione del progetto alla gestione dell'iniziativa e rendicontazione finale delle spese sostenute;
9) Gestione dei rapporti/ispezioni con l'Amministrazione Finanziaria (in particolare: Agenzia delle Entrate o Guardia di Finanza): si tratta dell'attività relativa alla gestione delle visite ispettive in materia fiscale;
10) Gestione dei flussi finanziari: l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività dell'Ente, in particolare agli incassi e pagamenti;
11) Gestione attiva degli omaggi, liberalità e sponsorizzazioni: si tratta dell'attività di spesa relativa a omaggi e liberalità e sponsorizzazioni (fiere, convegni, ecc.) per la promozione dell'immagine e dei corsi di Tao Group S.r.l.

SEZIONE 2 - LE FATTISPECIE DI REATI INFORMATICI E IL TRATTAMENTO ILLECITO DI DATI RICHIAMATE DALL'ART. 24 BIS DEL DECRETO.

L'art. 24–bis è stato introdotto, nel corpo del D. Lgs. n. 231/2001, dalla L. n. 48/2008, di ratifica della c.d. Convenzione Cybercrime, firmata a Budapest il 23 novembre 2001. L'introduzione di tale tipologia di reati nel novero delle fattispecie idonee a generare la

responsabilità dell'ente non è privo di conseguenze pratiche, constatato che l'uso di strumenti informatici è diffuso in ogni realtà aziendale.
L'art. 1 della citata Convenzione stabilisce che per "sistema informatico" deve intendersi qualsiasi dispositivo o qualsiasi gruppo di dispositivi tra loro interconnessi o collegati, uno o più dei quali, in base ad un programma, eseguono l'elaborazione automatica dei dati.

La principale caratteristica di un "sistema informatico" è, dunque, l'esecuzione automatizzata di operazioni. Per "dato informatico", la stessa Convenzione intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che ne permetta l'elaborazione con un sistema informatico. Tale definizione fa riferimento sia ai dati in senso stretto, sia ai programmi, in quanto i primi costituiscono le informazioni che vengono generate e salvate attraverso l'utilizzazione dei secondi.

- **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.); Documenti informatici**

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".
L'art. 491-bis c.p. fornisce una definizione di documento informatico basata sull'elemento materiale del supporto di memoria e non sui dati in esso contenuti: può definirsi supporto informatico qualsiasi supporto di memoria – sia esso interno sia esso esterno all'elaboratore elettronico – sul quale possono essere registrati e conservati per un certo periodo di tempo dei dati destinati ad essere letti ed eventualmente elaborati da un sistema informatico.
Non costituisce supporto informatico ai sensi dell'art. 491-bis c.p. il tabulato emesso dal computer al termine del processo di elaborazione: il tabulato – così come ogni output stampato – è infatti normalmente costituito da un foglio di carta sul quale il contenuto dei dati è riprodotto in caratteri alfanumerici per consentirne la lettura da parte dell'uomo; rientrano invece nella nozione di documento informatico le carte di pagamento a banda magnetica e le carte a microprocessore (ad es. carte prepagate, carta Viacard a scalare e alcune carte telefoniche).
È inoltre documento informatico il supporto informatico che contenga il programma specificamente destinato ad elaborare i dati, ossia il programma memorizzato all'interno del sistema informatico o su un supporto esterno che svolga la funzione di elaborare dati.

- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.).**

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".
Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico.
In particolare, per sistema informatico, ai fini della configurabilità del delitto di cui all'art. 615-ter c.p., deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche. Il sistema è dunque tale se gestisce ed elabora dati, mentre tutto ciò che in un sito web o nel mondo dell'informatica non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è sistema informatico.
L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, ossia tutte quelle misure di protezione al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema, quali a titolo esemplificativo codici di accesso, alfabetici o numerici da digitare su una tastiera o memorizzati su una banda magnetica di una tessera da introdurre in apposito lettore. Oltre a queste misure logiche possono rilevare anche misure fisiche quali l'uso di chiavi metalliche per l'accensione dell'elaboratore. La condotta rilevante consiste nell'introdursi abusivamente in un sistema protetto o nel permanervi contro la volontà espressa o tacita del titolare del diritto di escludere gli altri dall'uso del sistema. Si ha introduzione quando si oltrepassano le barriere

logiche e/o fisiche che presidiano l'accesso alla memoria interna del sistema e si è quindi in condizione di richiamare i dati ed i programmi che vi sono contenuti. L'introduzione può avvenire sia da lontano ossia per via elettronica sia da vicino da parte di chi si trovi a diretto contatto con l'elaboratore.
Oltre all'introduzione rileva anche l'ipotesi del mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare dello ius excludendi: tale caso ricorre quando, in seguito ad un'introduzione involontaria o causale o solo inizialmente autorizzata, l'agente permanga nel sistema informatico altrui nonostante il dissenso del soggetto che ha interesse alla riservatezza dei dati e dei programmi in esso contenuti.
È bene precisare che per operatore di sistema deve intendersi solo quella particolare figura di tecnico dell'informatica (c.d. system administrator) che all'interno di un'azienda ha il controllo delle diverse fasi del processo di elaborazione dati nonché la possibilità di accedere a tutti i settori della memoria del sistema informatico su cui opera, oppure di altri sistemi, qualora vi sia un collegamento in rete.

➢ **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.).**

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.
La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater".
L'art. 615-quater è rivolto a punire la condotta di detenzione e di diffusione abusiva di codici di accesso che può portare alla commissione di altri reati informatici: infatti chi entra in possesso abusivamente di codici d'accesso, può commettere un accesso abusivo ad un sistema o può diffondere tali codici ad altre persone che a loro volta potrebbero accedere abusivamente al sistema.
L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo: può infatti trattarsi di una password, di un codice d'accesso o semplicemente di informazioni che consentano di eludere le misure di protezione.
La disposizione in esame incrimina due tipi di condotte volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui oppure a procurare ad altri tali mezzi o comunque le informazioni sul modo di eludere le barriere di protezione; a contrario,

non è punita la semplice detenzione di codici di accesso o di strumenti similari da parte di chi non sia autorizzato a farne uso.

➢ **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.).**

"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro".

L'art. 615-quinques c.p. è rivolto a tutelare il patrimonio informatico, inteso come hardware, software e dati da attacchi con virus informatici.

La condotta punita è la diffusione (divulgazione), la comunicazione (portare a conoscenza) o la consegna (dare in senso materiale) di un programma informatico che ha lo scopo o l'effetto di danneggiare il sistema informatico o telematico altrui, o di danneggiare dati o programmi in esso contenuti o ad esso pertinenti, oppure l'interruzione parziale o totale del suo funzionamento o la sua alterazione.

La legge non fa distinzione tra virus creati da chi commette il reato o da terzi, né tanto meno tra programma informatico che reca concretamente un danno al sistema informatico e quello che non lo provoca.

Un programma può essere definito infetto ai sensi della disposizione in esame se è in grado non solo di danneggiare le componenti logiche di un sistema informatico, ma anche di interrompere o alterare il funzionamento di quest'ultimo.

➢ **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.).**

"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato".
Ai sensi della disposizione in esame la condotta può consistere alternativamente nell'intercettare fraudolentemente una comunicazione informatica o telematica oppure nell'impedirla o interromperla; il secondo comma prevede poi l'ipotesi della rivelazione in tutto o in parte mediante qualsiasi mezzo di informazione al pubblico del contenuto di una conversazione intercettata.
Intercettare una comunicazione informatica o telematica significa prendere cognizione del suo contenuto, intromettendosi nella fase della sua trasmissione; l'intercettazione deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso (ad es. decodificando dei dati trasmessi in forma cifrata o superando delle barriere logiche poste a difesa del sistema che invia o riceve la comunicazione) o comunque in modo tale da rendere non percepibile o riconoscibile a terzi l'intromissione abusiva.
La comunicazione è, invece, impedita quando se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati; una comunicazione può essere interrotta sia agendo sul sistema che invia e che deve ricevere la comunicazione sia ad esempio deviando il flusso dei dati in corso di trasmissione da un elaboratore ad un altro.

- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.).**

"Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.
Tale disposizione mira a reprimere una condotta antecedente e preparatoria rispetto a quella prevista dall'art. 617- quater c.p., vietando l'installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
Il reato previsto dall'art. 617-quinquies c.p. è stato ravvisato nel caso di utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico

dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione, con il sistema rientra nella nozione di "intercettare" di cui alla norma incriminatrice.

➢ **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.).**

"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

Oggetto del danneggiamento può essere innanzitutto un sistema informatico di qualsiasi tipo e dimensione, eventualmente collegato a distanza con altri elaboratori come nel caso dei sistemi telematici. L'aggressione può rivolgersi tanto al sistema nel suo complesso, quanto a una o più delle sue componenti materiali, quali a titolo esemplificativo le periferiche. Non possono invece essere considerati componenti di un sistema informatico i supporti magnetici o ottici sui quali non siano memorizzati dati o programmi, in quanto il loro danneggiamento non arreca nessun pregiudizio alla funzionalità del sistema informatico nel quale dovrebbero essere utilizzati.

Oltre al sistema informatico il danneggiamento può avere ad oggetto dati e programmi informatici; per dati si intendono quelle rappresentazioni di informazioni o di concetti che, essendo destinate alla elaborazione da parte di un computer, sono codificate in una forma (elettronica, magnetica ottica o similare) non percettibile visivamente. Suscettibili di danneggiamento possono essere anche dati o programmi immagazzinati nella memoria interna dell'elaboratore, oppure su un supporto esterno come un disco magnetico o ottico.

Tra i beni suscettibili di danneggiamento l'art. 635-bis c.p. indica anche le informazioni: poiché l'informazione è un'entità di per sé astratta, questa espressione assume significato solo in quanto la si riferisca alle informazioni incorporate su un supporto materiale, cartaceo o di altro tipo.

Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e la inservibilità totale o parziale. L'ipotesi di distruzione di dati e programmi più frequente e significativa è rappresentata dalla loro cancellazione: sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con nuovi dati diversi, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa. Poiché la distruzione deve essere totale, non ricorre questa ipotesi quando i dati o i programmi cancellati siano ancora recuperabili in una zona remota dell'elaboratore,

utilizzando un determinato tipo di programma oppure ne sia stata solo impedita la visualizzazione sullo schermo del computer.

➢ **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.).**

"Salvo che il fatto costituisca un più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

➢ **Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.).**

"Salvo che il fatto costituisca più grave reato, chiunque mediante le condotte di cui all'art. 635 bis c.p. ovvero

attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata.

➢ **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.).**

"Se il fatto di cui all'art. 635-quater c.p. è diretto a distruggere, danneggiare, rendere in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso in tutto o in parte inservibile la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Cfr. precedenti fattispecie.

2.1. ATTIVITA' SENSIBILI IN RELAZIONE AI REATI INFORMATICI E ALLA VIOLAZIONE DELLA PRIVACY.

L'art. 6 del Decreto indica quale elemento essenziale del Modello di Organizzazione, Gestione e Controllo l'individuazione delle cosiddette "attività sensibili" ovvero quelle attività aziendali che presentano il rischio della commissione di uno dei reati tassativamente indicati dal Decreto 231.

L'analisi condotta ha consentito di individuare quali attività presentino dei rischi con riferimento alla commissione dei predetti reati informatici. Per una corretta individuazione e inquadramento del rischio sono state mappate le apparecchiature informatiche esistenti e introdotta ai fini della 231 una regolamentazione anche in ordine all'accesso alle stesse.

In particolare,

- nella sede di Chianciano sono presenti diversi pc fissi con postazioni assegnate ai dipendenti/collaboratori (in tutto sono 10 postazioni);
- nella sede di Milano sono presenti diversi pc fissi con postazioni assegnate ai dipendenti/collaboratori (per un totale di 5 postazioni)
- tutti i pc sono protetti da password di accesso ad uso esclusivo che viene rinnovata ogni mese;
- le password sono custodite adottando le opportune regole di sicurezza atte a garantirne la riservatezza;
- tutti i pc possono connettersi alla rete internet tramite cavo Ethernet/WiFi e utilizzare la posta elettronica;
- sui vari pc sono caricati i programmi necessari per lo svolgimento dell'attività lavorativa dell'Ente (fra cui il pacchetto Office)
- alcuni pc montano sistema operativo Macintosh (per i commerciali), il pc del RSI monta sistema operativo Windows mentre per marketing e grafica Windows;
- tutti i pc si connettono ad Internet tramite router;
- tutti i software dalle postazioni fisse di Pc sono caricati dal RSI che ne cura l'acquisto di licenze e aggiornamenti;
- la configurazione dei pc è effettuata dal RSI;
- la società ha stipulato contratti con enti terzi che gestiscono l'archiviazione dei dati su server di loro proprietà;
- i dati che vengono trattati non vengono salvati sui pc ma direttamente in cloud;
- sono applicate restrizioni sia sulla possibilità di scaricare software diversi sia per l'accesso a siti internet qualificati come black list per impedirne l'accesso.

Si è proceduto, poi, ad individuare le attività svolte dall'Ente Tao che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione di reati richiamati dagli articoli indicati in questa sezione.
Le aree di rischio sono da individuarsi nelle attività sensibili qui di seguito individuate:

1) gestione profili utente e autenticazione;
2) gestione e protezione della postazione lavorativa;
3) gestione degli accessi da e per l'esterno;
4) gestione e protezione dei dati particolari;
5) gestione e protezione delle reti;
6) gestione dei contratti che consentono di scaricare il rischio sul terzo;
7) sicurezza fisica (sicurezza cablaggi, dispositivi di rete etc..).

All'esito dell'analisi sono stati apportati dei correttivi che consentano una maggior tutela dei dati particolari trattati, in ottemperanza alla normativa sulla privacy.
In particolare;

- la predisposizione di informative dove viene separato il c.d. consenso "obbligatorio" da quello "facoltativo";
- il rilascio, da parte di ogni discente, di liberatoria per consentire l'eventuale pubblicazione della propria immagine personale sui siti internet dell'organizzazione.

SEZIONE 3 - LE FATTISPECIE IN TEMA DI REATI SOCIETARI.

L'art. 25-ter del D. Lgs. n. 231/2001 introduce la responsabilità amministrativa della persona giuridica con riferimento alla maggior parte dei reati societari.
Nel novero di detti reati, è ravvisabile l'interesse del legislatore finalizzato ad assicurare la trasparenza nella gestione societaria, la corretta tenuta dei documenti contabili, la corretta informazione ai terzi, a tutelare il capitale sociale, il patrimonio sociale, il regolare funzionamento dell'Ente, le funzioni di controllo.
Si elencano qui di seguito le fattispecie contemplate dall'art. 25-ter del Decreto che possono assumere rilevanza in relazione a Tao Group S.r.l.

➢ **False comunicazioni sociali (art. 2621 – 2621 bis – 2621 ter c.c.) e false comunicazioni sociali in danno della Società, dei soci o dei creditori (art. 2622 c.c.).**

La consumazione di questi reati avviene con l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette alle competenti autorità o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni ovvero omettendo

informazioni imposte dalla legge, in modo idoneo ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria dell'Ente, con l'intenzione di ingannare i soggetti destinatari di cui sopra.
La condotta deve essere finalizzata a conseguire per sé o per altri un ingiusto profitto.
La responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dall'Ente per conto di terzi.
Ai fini della punibilità, le informazioni false o omesse devono alterare "in modo sensibile la rappresentazione della situazione economica patrimoniale o finanziaria dell'Ente e la condotta deve comunque determinare una variazione superiore al 5% del risultato economico di esercizio, al lordo delle imposte, o una variazione superiore all'1% del patrimonio netto".
Qualora le alterazioni siano inferiori alle soglie sopra indicate, sono comunque previste sanzioni amministrative pecuniarie e sanzioni interdittive nei confronti delle persone fisiche che hanno posto in essere la condotta.
Il reato di cui all'art. 2622 c.c. richiede l'ulteriore circostanza che le informazioni, false od omesse, abbiano cagionato un danno patrimoniale all'Ente e ai creditori.
Nel caso prescritto dall'art. 2621 c.c. sono previste ipotesi attenuate per fatti di lieve entità in base alla natura e alle dimensioni della società oltre che alle modalità e agli effetti della condotta. E' prevista, altresì, la possibilità di una pronuncia ai sensi dell'art. 131 bis c.p. per lieve entità del fatto.

- **Indebita restituzione dei conferimenti (art. 2626 c.c.)**

Con tale fattispecie viene punito l'amministratore che, fuori dai casi di legittima riduzione del capitale sociale, restituisce anche simulatamente, i conferimenti ai soci o li libera dall'obbligo di eseguirli.

- **Operazioni in pregiudizio dei creditori (ast. 2629 cc)**

Anche la predetta fattispecie punisce l'amministratore che effettua operazioni (riduzione del capitale sociale o fusioni con altre società o scissioni) violando le disposizioni che tutelano gli interessi dei creditori e cagionando danno a costoro. Il reato è procedibile a querela della persona offesa, tuttavia, il risarcimento integrale del danno ai creditori prima del giudizio estingue il reato.

3.1. ATTIVITA' SENSIBILI IN RELAZIONE AI REATI SOCIETARI.

Le attività valutate potenzialmente "sensibili" in riferimento ai citati reati societari sono connesse ai vari adempimenti che Tao Group è tenuta ad ottemperare e che riguardano:

- la tenuta della contabilità;
- la formazione e redazione del bilancio e/o di ogni comunicazione sociale;
- la formazione e redazione delle relazioni, atti e comunicazioni previste dalle singole disposizioni di legge, relative alla situazione economica, patrimoniale o finanziaria dell'Ente;
- attività di revisione contabile;
- disposizioni dei beni sociali;
- conservazione e tenuta della documentazione contabile ai fini di consentire l'eventuale attività di controllo o di revisione normativamente previste;
- svolgimento del CDA, formazione della volontà nel CDA e verbalizzazione;
- rapporti tra i vari organi interni.

SEZIONE 4 – LE FATTISPECIE DI REATO IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO.

La legge 3 agosto 2007 n. 123 ha aggiunto nel D. Lgs. n. 231/2001 l'art. 25-septies, successivamente sostituito dall'art. 300 D. Lgs. n. 81/2008.
Con tale intervento sono stati previsti tra i reati presupposto per l'applicazione del D. Lgs. n. 231/2001 anche l'omicidio colposo e le lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. Tali reati vengono considerati rilevanti ai fini del D. Lgs. n. 231/01 qualora la violazione delle norme antinfortunistiche sia finalizzata ad un risparmio economico o anche semplicemente di tempo.
La finalità perseguita è quella di introdurre una maggior tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi in modo da ridurre il fenomeno degli infortuni sul lavoro.
Le due fattispecie puniscono la condotta di chi cagiona per colpa, rispettivamente, la morte oppure una lesione personale grave o gravissima.
Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita e provochi l'incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo.
Per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Le fattispecie del reato sono le seguenti:

- **Omicidio colposo (art. 589 c.p.).**

"1. Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.
2. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.
3. [...]
4. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

- **Lesioni personali colpose (art. 590 c.p.).**

"1. Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.
2. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.
3. Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.
[...]
4. Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.
5. Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale."

Nel caso di commissione, nell'interesse o a vantaggio dell'Ente, di talune delle fattispecie considerate, qualora il fatto si verifichi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul luogo di lavoro, anche l'Ente viene chiamato a risponderne ai sensi del D. Lgs. 231/2001.
Il regime sanzionatorio applicabile per i reati in materia di salute e sicurezza sul lavoro è di natura sia pecuniaria che interdittiva.
In relazione al delitto di cui all'articolo 589 del codice penale, se commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3

agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote.
Qualora il delitto di cui all'articolo 589 del codice penale, sia commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote.
In entrambe le ipotesi relative alla commissione del delitto di cui all'articolo 589 è prevista l'applicazione di sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.
In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Sono inoltre applicabili le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi.

4.1. ATTIVITA' SENSIBILI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO.

L'art. 6 del Decreto indica quale elemento essenziale del Modello di Organizzazione, Gestione e Controllo l'individuazione delle cosiddette "attività sensibili" ovvero quelle attività aziendali che presentano il rischio della commissione di uno dei reati tassativamente indicati dal Decreto 231.
L'analisi condotta ha consentito di individuare quali attività presentino dei rischi con riferimento alla commissione dei predetti reati indicati dall'art. 25-septies del Decreto. L'elenco completo ed esaustivo delle attività a rischio, delle misure di prevenzione e protezione adottate e il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei presidi di sicurezza è contenuto nel Documento di Valutazione dei Rischi (DVR) a norma del D. Lgs. 81/2008 a cui si rimanda.
Le attività "sensibili" riferite ai reati in materia di salute e sicurezza sul lavoro sono potenzialmente presenti in ogni ambito e attività lavorativa.
Nel caso specifico di Tao Group S.r.l. i suddetti reati potrebbero, astrattamente, essere commessi in tutti i casi in cui si verifichi una violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Nell'ambito della propria attività il Responsabile Salute e Sicurezza sul Lavoro preposto potrebbe rispondere di omicidio colposo e/o lesioni personali colpose.
Di seguito si elencano le principali attività sensibili, sebbene il rischio sia basso:

- circolazione persone all'interno delle aule e degli spazi dedicati alla didattica;
- ribaltamento di mobilia;
- schiacciamento;
- aggressioni fisiche e verbali;

- reazioni allergiche da prodotti per massaggio;
- fiamme ed esplosioni.

SEZIONE 5 - LE FATTISPECIE DI REATO RICHIAMATE DALL'ART. 25-OCTIES DEL DECRETO.

Il D. Lgs. n. 231/2007 ha introdotto nel D. Lgs. 231/2001 l'art. 25-octies che, per quanto interessa, aggiunge i delitti di ricettazione e riciclaggio all'elenco degli illeciti presupposto della responsabilità degli Enti.
Qui di seguito si descrivono sinteticamente i reati di ricettazione e riciclaggio cui si riferisce l'art. 25-octies D. Lgs. n. 231/2001.

➢ Ricettazione (art. 648 c.p.).

Il reato di ricettazione persegue la tutela del patrimonio (secondo alcuni autori, l'interesse tutelato è anche quello dell'amministrazione della giustizia) ed è punito dall'art. 648 c.p., a mente del quale:
"1. Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.
2. La pena è della reclusione sino a sei anni e della multa sino a euro 516, se il fatto è di particolare tenuità.
3. Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto."

➢ Riciclaggio (art. 648-bis c.p).

Il reato di riciclaggio si presenta come plurioffensivo, in quanto persegue la tutela del patrimonio, dell'amministrazione della giustizia e, a seconda della fattispecie, anche dell'ordine pubblico ed economico.
La disposizione cui fare riferimento in tema di riciclaggio è l'art. 648-bis c.p., secondo cui:
"1. Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.
2. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

3. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita le pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648."

5.1. ATTIVITA' SENSIBILI IN MATERIA DI RICETTAZIONE E RICICLAGGIO.

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno degli elementi essenziali dei Modelli di Organizzazione, Gestione e Controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001.

L'analisi svolta nel corso del Progetto per l'adozione del Modello e, successivamente, durante la sua applicazione ed implementazione nel tempo, ha permesso di individuare le attività di Tao Group che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'art 25-quinquies (Delitti contro la personalità individuale), e art. 25-octies (reati di ricettazione, riciclaggio, impiego di denaro, beni o altra utilità di provenienza illecita) ex D. Lgs. 231/2001.

Qui di seguito sono elencate le attività sensibili.

- Gestione delle risorse informatiche (accesso Internet ed uso della posta elettronica)

Si tratta delle modalità di utilizzo delle risorse informatiche dell'Ente da parte dei soggetti ad esso appartenenti.

Particolare attenzione deve essere dunque posta proprio nell'utilizzo dei P.C. ai quali è consigliabile accedere sempre con una propria password identificativa.

- Gestione dei flussi finanziari.

Si tratta delle attività di gestione di incassi e pagamenti nei confronti di fornitori per acquisto di beni o prestazioni di servizio.

- Gestione dei contratti con soggetti terzi per l'affidamento di servizi.

Si tratta della gestione del rapporto con società terze cui viene affidato lo svolgimento di servizi (es. impresa di pulizie e di ristorazione) e dell'attività di gestione sito internet e sistema gestionale.

In via generale le attività "sensibili" riferite ai reati in materia di ricettazione e riciclaggio sono potenzialmente presenti ogni qualvolta vi siano movimentazioni di somme o acquisiti di beni.

Nel caso specifico nell'Ente Tao Group S.r.l., le attività relative ai pagamenti sono ravvisabili:

- nelle operazioni di cassa per il pagamento dei corsi;
- nell'acquisto di beni necessari all'attività di insegnamento (prodotti per il massaggio, asciugamani, materiale per i corsi etc)

- pagamento dei fornitori;
- vendita anche tramite e-commerce di prodotti per il massaggio (creme, oli, lettini, biancheria da massaggio etc..)

SEZIONE 6 - FATTISPECIE IN MATERIA DI DIRITTI D'AUTORE.

La legge n. 99 del 2009 ha inserito tra i reati presupposto ex d. lgs. 231 una serie di fattispecie contenute nella c.d. "legge sul diritto d'autore" (legge 22 aprile 1941 n. 633).
Il nuovo articolo 25-novies prevede per l'ente sanzioni pecuniarie che possono arrivare fino a euro 516,00 e sanzioni interdittive per la durata massima di un anno.
Analizziamo qui di seguito le fattispecie previste dal nuovo articolo 25-novies.

➢ ART. 171 CO. 1 LETT. A BIS) E CO. 3 DELLA LEGGE SUL DIRITTO D'AUTORE.

Delle numerose norme contenute in questo articolo, vengono inseriti come reati-presupposto solo la lettera a) bis del primo comma e il terzo comma dell'articolo.
Il primo delitto, introdotto dalla legge n. 43 del 2005, punisce la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa.
In questa norma ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.
L'inserimento del delitto nel D. Lgs. n. 231/2001 risponde quindi ad una visione politica di responsabilizzazione di tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d'autore.
Tao Group S.r.l., per contenere il rischio di tale reato, dovrà predisporre controlli più accurati sui contenuti che "transitano" sui propri server. Ciò, a stretto rigore, anche qualora siano gli utenti stessi a "postare" i contenuti direttamente e senza filtro preventivo del gestore (si pensi al sistema di funzionamento di YouTube); anche in questi casi si potrebbe configurare una responsabilità per la società, che non si è organizzata per prevenire tale rischio di reato.
Il delitto di cui al comma 3 punisce le condotte sopra menzionate ove commesse su una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.
In quest'ultima fattispecie di danno il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

➢ ART. 171-BIS DELLA LEGGE SUL DIRITTO D'AUTORE.

"1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banda di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità."

La disposizione, introdotta dal D. Lgs. n. 489 del 1992, di attuazione della Direttiva 91/250/CE, ha segnato l'ingresso nel panorama normativo italiano della tutela penale del software.

Da notare, però, che la disposizione non contiene alcuna definizione del proprio oggetto di tutela: il software. Per ricostruirne l'esatta portata è allora necessario far riferimento alle disposizioni civilistiche contenute nella medesima legge.

In particolare, l'art. 2 della legge sul diritto d'autore tutela "*i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso.* "

L'articolo si divide in due commi: il primo volto alla tutela dei software in generale, il secondo, inserito dal D. Lg. 169/99 tutela le banche dati.

Quanto al primo comma, la disposizione colpisce la condotta di abusiva duplicazione: il legislatore si è mostrato più rigoroso di quello europeo, che, invece, riteneva necessaria la punibilità solo di condotte più propriamente finalizzate al commercio. Ad oggi, quindi, è prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro, accezione ben più ampia della versione precedente, che prevedeva la presenza del dolo specifico di profitto.

A restringere l'ambito di applicabilità della norma vi è, però, il riferimento all'abusività della riproduzione che, sul piano soggettivo implica che il dolo dell'agente debba ricomprendere anche la conoscenza delle norme extra-penali che regolano la materia.
La seconda parte del comma elenca le condotte di importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "piratati"; sono tutte condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.
Infine, nell'ultima parte del comma il legislatore ha inteso inserire una norma volta all'anticipazione della tutela penale, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Sul piano soggettivo, tutte le condotte ora esaminate sono caratterizzate dal dolo specifico di profitto.
Con la novella del 2000 il legislatore, nel sostituire il fine di profitto a quello di lucro, ha inteso ampliare l'ambito di applicazione della norma, per ricomprendervi anche quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico.
La riforma dell'elemento soggettivo avrà forti ricadute sull'eventuale punibilità dell'Ente, posto che, in tal modo, si può configurare il reato anche qualora, all'interno di una struttura, vengano usati, a scopi lavorativi, programmi non originali, al solo fine di risparmiare il costo dei software originali.
Nel secondo comma dell'art. 171-bis ad essere tutelate sono invece le banche dati; per esse intendendosi, stando all'art. 2 della stessa legge, le "raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo".
Anche a questo secondo comma devono prudentemente prestare attenzione le aziende che, per le più svariate ragioni, gestiscono banche dati.

- **ART. 171-TER DELLA LEGGE SUL DIRITTO D'AUTORE.**

"1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:
a) [..];
b) Abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) Pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) Detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) In assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) Introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
f-bis) fabbrica, importa distribuisce, vende noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;
Abusivamente rimuove o altera le informazioni elettroniche di cui all'art. 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.
2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:

a) Riproduce, duplica trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) Esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) Promuove o organizza attività illecite di cui al comma 1.
3. la pena è diminuita se il fatto è di particolare tenuità.
4. La condanna per uno dei reati previsti nel comma 1 comporta:
a) L'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) La pubblicazione della sentenza in uno o più quotidiano, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) La sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.
5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.".
La lunga disposizione tende alla tutela di una serie numerosa di opere dell'ingegno: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche.
Le numerose condotte sanzionate, che qui non vengono analizzate per ragioni di spazio, si inseriscono nell'ottica di una pretesa "penalizzazione" che il legislatore degli ultimi anni ha perseguito nei confronti della tutela del software.
A restringere l'ambito di applicabilità della disposizione, però, vi sono due requisiti.
Il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno; il secondo è il dolo specifico di lucro, necessario per integrare il fatto tipico.
A seguito della novella di cui alla legge 99 del 2009, molte saranno le aziende che potranno essere esposte ad un procedimento penale: aziende di telecomunicazioni, cinematografiche, società che gestiscono spettacoli teatrali e simili.

- **ART. 171-SEPTIES DELLA LEGGE SUL DIRITTO D'AUTORE.**

"1. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza e assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici".
La disposizione in esame è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto d'autore. Si tratta pertanto di un reato di ostacolo che si consuma con la mera violazione dell'obbligo.
La disposizione estende la pena prevista dal primo comma dell'art. 173-bis ai produttori e agli importatori dei supporti non soggetti al contrassegno SIAE che non comunichino alla SIAE stessa entro trenta giorni dall'importazione o dalla commercializzazione i dati necessari all'univoca identificazione dei supporti medesimi.
Il secondo comma punisce, invece, la falsa comunicazione di tali dati alla SIAE.
Come in altri settori, quindi, si è voluta accordare una tutela penale alle funzioni di vigilanza delle Autorità preposte al controllo del settore.
Nell'ottica 231, l'Ente dovrà implementare nel modello specifiche misure volte a regolamentare lo scambio informativo con la Società Italiana Autori ed Editori (SIAE).

- **ART. 171-OCTIES DELLA LEGGE SUL DIRITTO D'AUTORE.**

"1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio
2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità".
La disposizione punisce chi, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica utilizza per uso pubblico o privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.
L'articolo, poi, continua definendo ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.
Vale a restringere l'ambito di applicabilità della norma l'elemento soggettivo di perseguimento di fini fraudolenti.

6.1. ATTIVITA' SENSIBILI IN RELAZIONE AI REATI IN MATERIA DI DIRITTO D'AUTORE.

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno degli elementi essenziali dei Modelli di Organizzazione, Gestione e Controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001 relativi al diritto d'autore.
L'analisi condotta sull'Ente Tao Group ha consentito di individuare le attività che potrebbero essere ritenute "sensibili" in un'ottica di valutazione del rischio di commettere i reati richiamata nell'art. 25-nonies del Decreto.
Di seguito l'elenco delle attività considerate sensibili.

- **Gestione dei rapporti con le società fornitrici di prodotti informatici in relazione al rilascio del contrassegno SIAE e al pagamento dei diritti d'autore.**
  Ci si riferisce a quelle attività relative ai soggetti che acquistano prodotti informatici e delle modalità con cui sono regolati gli adempimenti relativi ai diritti d'autore.
- **Gestione, acquisto e utilizzo di licenze software da dedicare all'attività d'impresa.**
  Trattasi del rischio derivante dall'acquisto, installazione, gestione e rinnovo dei sistemi operativi che dei software applicati ai vari pc della Tao Group.
- **Gestione e diffusione del materiale didattico relativo ai corsi di formazione proposti da Tao Group.**
  L'attività d'insegnamento prevede che l'Ente direttamente fornisca, sia in copia informatica/digitale che in versione cartacea, i manuali di testo di proprietà dell'Ente stesso, che ne cura la stesura e l'aggiornamento.
- **Gestione e regolamentazione della vendita anche tramite e-commerce dei prodotti con marchio Tao Group.**
  La vendita di prodotti a marchio Tao Group può configurare il rischio di contraffazione di prodotti.

SEZIONE 7 – LE FATTISPECIE DI REATO CONTRO LA FEDE PUBBLICA E CONTRO L'INDUSTRIA E IL COMMERCIO (art. 25-BIS / 25-BIS.*1*).

La presente sezione ha ad oggetto sia i delitti contro la fede pubblica che quelli contro l'industria e il commercio, in considerazione dell'affinità delle rispettive aree considerate "a

rischio reato", ovvero dei settori e/o dei processi dell'Ente Tao Group rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati, nonchè dei sistemi di controlli implementati.
L'analisi delle attività svolte dall'organizzazione ha consentito di individuare le aree c.d. a rischio di commissione dei reati in argomento e riguardano principalmente la gestione della comunicazione al pubblico e la vendita dei prodotti relativi al benessere e ai massaggi.
Si fornisce, di seguito, una breve descrizione dei reati rilevanti ai fini del D. Lgs. n. 231/200:

7.1. I DELITTI CONTRO LA FEDE PUBBLICA.

➢ **Art. 473 c. p. - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni.**

Commette questo reato chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi, segni distintivi, sia nazionali che esteri, di prodotti industriali, brevetti, disegni e modelli industriali.
Commette, altresì, il reato in esame chiunque, anche se non partecipa attivamente alla contraffazione o all'alterazione, fa uso di tali marchi, segni distintivi o brevetti contraffatti.
Affinché la fattispecie possa considerarsi realizzata, è necessario, peraltro, che i marchi, i segni distintivi, i brevetti, disegni e modelli, siano stati regolarmente registrati o brevettati, secondo le norme interne o le convenzioni internazionali.
La giurisprudenza ha indicato che si può intendere l'attività di contraffazione, in tema di marchi, come quelle operazioni che «fanno assumere al marchio falsificato caratteristiche tali da ingenerare confusione sulla autentica provenienza del prodotto, con possibile induzione in inganno dei compratori», mentre l'alterazione può essere considerata come una più semplice modificazione parziale di un marchio registrato, che viene ottenuta mediante l'eliminazione o aggiunta di elementi costitutivi marginali, in cui, peraltro, possono anche essere incluse le condotte di imitazione di marchi genuini. La stessa giurisprudenza, peraltro, ritiene, comunque, che in entrambe le condotte esposte l'imitazione che si pone in essere debba essere di un elevato livello, in mancanza del quale, si ritiene, non possa esserci lesione della buona fede del consumatore, bene che la norma mira a tutelare.
Per il caso dei brevetti, invece, la giurisprudenza considera integrata la condotta di "contraffazione" non solo quando c'è una «riproduzione pedissequa del prodotto o del procedimento per i quali è stato concesso il brevetto» ma anche quando solamente non sia presente una «idea inventiva priva del carattere di concreta novità» e che si limiti a «riprodurre mediante soluzioni banali e ripetitive la struttura generale oggetto del brevetto, non apportando alcun elemento di concreta novità».

In relazione, invece, al significato di uso di marchi, segni distintivi o brevetti contraffatti, deve intendersi l'apposizione del marchio o del segno distintivo su un determinato prodotto, ovvero lo sfruttamento dell'opera dell'ingegno tutelata da brevetto.
Con l'introduzione, nella riformulazione dell'articolo del 2009, della locuzione "potendo conoscere l'esistenza del titolo di proprietà industriale", diventa necessario per le aziende, ogniqualvolta debbano registrare un marchio, logo o brevettare una qualsiasi opera dell'ingegno, compiere complete e penetranti ricerche sulla possibile esistenza anteriore di segni distintivi già registrati o opere dell'ingegno già brevettate.

- **Art. 474 c. p. - Introduzione nello Stato e commercio di prodotti con segni falsi.**

La condotta descritta dalla norma dispone una sanzione quando, al di fuori dei casi previsti dall'articolo precedentemente esaminato, si introducono nel territorio dello Stato per tranne profitto, si pongono in vendita sia in Italia che all'estero, si detengono per vendere, si mettono in altro modo in circolazione prodotti industriali con marchi o altri segni distintivi, sia nazionali che esteri, contraffatti o alterati, al fine di trarre profitto.

Anche per quanto riguarda questo reato, è necessario che i marchi e i segni distintivi (contraffatti) siano regolarmente registrati ai sensi della normativa nazionale o internazionale. Affinché si integri la condotta del reato, è necessario che chi lo commette abbia come fine il raggiungimento di un "profitto". È da intendersi come "profitto" ogni vantaggio economico, o economicamente valutabile, che una persona, fisica o giuridica, può ottenere, in qualsiasi modo, anche, ad esempio, sotto forma di mancata spesa.

7.2. I DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO.

- **Art. 513 c. p. - Turbata libertà dell'industria o del commercio.**

Il reato in esame tutela il normale esercizio dell'attività industriale o commerciale, visto che punisce chiunque adoperi violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

- **Art. 513-bis c. p. - Illecita concorrenza con minaccia o violenza.** Tale fattispecie mira a punire chiunque, nell'ambito di un'attività commerciale, industriale o comunque produttiva, commetta atti di concorrenza, usando violenza o minacce. L'articolo prevede delle aggravanti qualora tali atti riguardino attività finanziate, anche solo parzialmente, dallo Stato o da altri enti pubblici.

- **Art. 514 c. p. - Frodi contro le industrie nazionali.**

Questo reato, punisce chi ponendo in vendita, o mettendo in altro modo in circolazione, prodotti industriali contrassegnati da marchi, nomi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale. Questa ipotesi, peraltro, dà rilievo non solo ai marchi e segni distintivi registrati secondo la normativa nazionale od internazionale, ma anche a quelli che non lo sono, sancendo, quindi, un'ampia protezione del bene tutelato.

➢ **Art. 517 c. p. - Vendita di prodotti industriali con segni mendaci.**

L'art. 517 c.p. punisce chiunque ponga in vendita, o metta altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, in modo da indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.

A differenza di quanto previsto dagli artt. 473 e 474 c.p., affinché il reato in esame venga ad esistenza, non è necessario che i nomi, i marchi, i segni distintivi industriali siano registrati secondo le normative nazionali ed internazionali. Il bene tutelato, in questo caso, non è la fede pubblica, come si è potuto riscontrare in molti dei reati esaminati, ma l'ordine economico in senso generale, e quindi il potenziale acquirente dei beni messi in commercio secondo le modalità esposte.

SEZIONE 8 – LE FATTISPECIE DI REATI TIBUTARI.

Per quanto concerne la presente Parte Speciale "G", si provvede, di seguito, a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 25 quinquesdecies del d.lgs. 231/2001 [articolo aggiunto dalla L. n. 157/2019 e dal D. Lgs. n. 75/2020], che si possono raggruppare in 2 tipologie di delitti, corrispondenti ad 8 distinte fattispecie criminose.

8.1. DELITTI IN MATERIA DI DICHIARAZIONE.

➢ **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D. Lgs. n. 74/2000).**

Il reato di dichiarazione fraudolenta mediante l'uso di fatture o di altri documenti per operazioni inesistenti è previsto e punito dall'art. 2, D.lgs. n. 74/2000, che punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni annuali relative a dette imposte elementi passivi fittizi. In tal caso, il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria. Per dette ipotesi, la fattispecie criminosa potrebbe

configurarsi nel caso in cui la Società riceva "fatture o altri documenti" a fronte di operazioni di acquisto di beni e servizi inesistenti, fatture che poi provvede a registrare nelle scritture contabili o comunque a detenere ai fini di prova nei confronti dell'Amministrazione finanziaria. In tal caso, il reato si perfeziona (ossia si reputa commesso) nel momento in cui l'Ente indica detti elementi passivi fittizi nella dichiarazione annuale. A tal fine si precisa, altresì, che la nozione di operazione inesistente appare particolarmente ampia, includendo: a) le operazioni mai effettuate (cosiddetta inesistenza oggettiva): che si verifica nel caso in cui l'Ente riceva una fattura di acquisto di un servizio o di un bene, che in realtà non ho mai acquistato; b) le operazioni effettuate, ma per le quali è stato indicato in fattura un importo diverso, generalmente superiore (cosiddetta sovrafatturazione): che si verifica nel caso in cui si acquisti un servizio o un bene per 100, ma per il quale ricevo una fattura di 600; c) le operazioni effettuate ma tra parti diverse (cosiddetta inesistenza soggettiva): che si verifica nel caso in cui l'Ente abbia realmente effettuato l'acquisto, ma il reale fornitore risulti diverso da quello indicato nella fattura. Nel caso di specie è stata introdotta un'attenuante specifica quando gli importi (per il medesimo periodo d'imposta) non superano gli euro 100.000.

- **Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. n. 74/2000)**.

Il delitto in esame è quello di cui all'art. 3, D. Lgs. n. 74/2000, che, fuori dai casi previsti dall'art. 2 (Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti), e quindi dall'impiego in dichiarazione di fatture false, punisce chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e a indurre in errore l'Amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 30.000 euro; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a 1.500.000 euro, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a 30.000 euro.

- **Dichiarazione infedele (art. 4 D. Lgs. n. 74/2000).**

Il delitto in esame è quello di cui all'art. 4, D. Lgs. n. 74/2000, che, fuori dai casi previsti dagli articoli 2 e 3 (per le dichiarazioni fraudolente), punisce il soggetto che, al fine di evadere le imposte dirette o l'Iva (senza un impianto fraudolento, ma comunque

consapevolmente e volontariamente), indica in una delle dichiarazioni annuali relative a queste imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi quando congiuntamente: a) l'imposta evasa è superiore a 100.000 euro con riferimento a ciascuna delle singole imposte;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione anche mediante indicazione di elementi passivi fittizi è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, comunque, è superiore a 2 milioni di euro; entrambi i parametri di cui sopra devono essere riferiti a ciascuna singola imposta. Non sono quindi penalmente rilevanti le condotte alle quali consegue il superamento della soglia di punibilità sommando gli importi delle due tipologie di imposte evase. Quest'ultima specificazione, che tiene conto del sistema della dichiarazione unica, esclude la sommatoria tra evasione concernente le imposte sui redditi ed evasione concernente l'imposta sul valore aggiunto; al tempo stesso, però, rende rilevante il superamento del limite anche quando si sia verificato in rapporto ad una soltanto delle imposte considerate. Il perfezionamento della fattispecie illecita in commento si realizza, dunque, mediante la presentazione di una dichiarazione annuale relativa alle imposte dirette e IVA, indicando in esse elementi attivi che manifestano una discrasia con quelli reali ovvero elementi passivi fittizi, determinando un'evasione d'imposta nei limiti indicati espressamente dal legislatore.

- **Omessa dichiarazione (art. 5 D. Lgs. n. 74/2000)**

L'omessa dichiarazione è un reato, previsto dall'art. 5 D. Lgs. 74/2000, che prevede due fattispecie criminose, punendo: a) con la prima (comma 1, dell'art. 5 in commento), chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto non presenta la dichiarazione ai fini delle imposte sul reddito o dell'Iva, pur essendovi tenuto, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila; b) con la seconda (comma 1-bis, dell'art. 5 in commento), chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila. Rispetto al delitto di dichiarazione infedele di cui all'art. art. 4 D. Lgs. n. 74/2000, la soglia di punibilità è più bassa, essendo sufficiente che l'imposta evasa (relativamente ad un'imposta) superi euro cinquantamila. Inoltre, ai sensi de ai sensi dell'articolo 5, comma 2, del D. Lgs. n. 74/2000, sono escluse dalla previsione penale: a) le dichiarazioni presentate entro 90 giorni dalla scadenza; b) le dichiarazioni non sottoscritte da persona legittimata o non redatte su stampati conformi a quelli ministeriali prescritti.

➢ **Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D. Lgs. n. 74/2000).**

La norma punisce la condotta di chi emette o rilascia fatture o altri documenti per operazioni inesistenti per consentire a terzi l'evazione delle imposte sui redditi o sul valore aggiunto. Se in riferimento al medesimo periodo d'imposta vengono emesse più fatture o documenti, si considera come un solo reato. La ratio della norma è quella di prevedere condotte simili a quelle descritte dall'art. 2 del codice tributario con la differenza che, nel caso di specie, chi agisce lo fa nell'interesse di altri soggetti. Anche in questo caso è prevista un'attenuante specifica per importi inferiori ad euro centomila.

8.2. DELITTI IN MATERIA DI DOCUMENTI E PAGAMENTO DI IMPOSTE.

➢ **Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D. Lgs. n. 74/2000).**

La condotta delittuosa in esame, emissione di fatture o altri documenti per operazioni inesistenti, è prevista dall' art. 8 D. Lgs. n. 74/2000 e si pone all'inizio di un percorso che condurrà, nella maggior parte dei casi, all'utilizzo di tali documenti falsi e quindi al concretizzarsi del reato di cui all'art. 2 - dichiarazione fraudolenta - realizzando appieno quel fine di consentire a terzi l'evasione. I citati reati sono infatti legati dall'unicità del fine, nel senso che il primo (art. 8) costituisce il mezzo normale per realizzare il secondo (art. 2): normalmente accade che chi emette la fattura falsa, intestandola a un certo soggetto (il potenziale utilizzatore) si è prima accordato con l'utilizzatore stesso, ovvero ha accolto la sua istigazione. In tale ambito l'art. 8 D. Lgs. n. 74/2000 in esame dispone che "E' punito con la reclusione da un anno e sei mesi a sei anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato". In tal caso, il reato si perfeziona (ossia si reputa commesso) all'atto dell'emissione o del rilascio della fattura o del documento per operazioni inesistenti. Benchè il rilascio o l'emissione di più fatture o documenti, nell'arco del periodo d'imposta, realizza un unico delitto, si ritiene che la consumazione del reato coincida con l'emissione o il rilascio del primo documento in ordine temporale; al contrario, il termine prescrizionale decorre dall'emissione dell'ultimo documento.

➢ **Occultamento o distruzione di documenti contabili (art. 10 D. Lgs. n. 74/2000).**

Il delitto in esame è quello di cui all'art. 10, D. Lgs. n. 74/2000, che, fuori dai casi in cui il fatto costituisca più grave reato (come, ad esempio, nel caso di bancarotta fraudolenta, o bancarotta semplice, etc..) punisce chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentirne l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari. La condotta sanzionata dall'art. 10 cit. è solo quella, espressamente contemplata dalla norma, di occultamento o distruzione (anche solo parziale) delle scritture contabili obbligatorie e non anche quella della loro mancata tenuta, espressamente sanzionata in via meramente amministrativa dall'art. 9 del d.lgs. n. 471 del 1997. In altre parole, la fattispecie criminosa dell'art. 10 presuppone l'istituzione della documentazione contabile. La condotta di occultamento di cui all'art. 10 del D. Lgs. 74/2000, consiste, dunque, nella indisponibilità della documentazione da parte degli organi verificatori, sia essa temporanea o definitiva. Il reato è integrato in tutti i casi in cui la distruzione o l'occultamento della documentazione contabile dell'impresa non consenta o renda difficoltosa la ricostruzione delle operazioni, rimanendo "escluso" solo quando il risultato economico delle stesse possa essere accertato in base ad altra documentazione conservata dall'imprenditore e senza necessità di reperire altrove elementi di prova. Al contrario, il reato non si configura se è possibile ricostruire il reddito e il volume d'affari tramite la documentazione restante che venga esibita o rintracciata presso la sede del contribuente oppure presso il suo domicilio ovvero grazie alle comunicazioni fiscali che il contribuente stesso (dichiarazioni dei redditi, dichiarazioni IVA, bilanci depositati) ha fatto all'Amministrazione Finanziaria.

- **Sottrazione fraudolenta al pagamento di imposte (art. 11 D. Lgs. n. 74/2000).**

La norma in commento prevede due fattispecie criminose, punendo:
a) con la prima (comma 1, art. 11 D. Lgs. n. 74/2000) tutti i soggetti che, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore, rispettivamente ad euro cinquantamila e/o duecentomila (limiti in ragione dei sia applica una differente sanzione penale), alienano simulatamente o compiono altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva;
b) con la seconda (comma 2, art. 11 D. Lgs. n. 74/2000) tutti i soggetti che, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indicano nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Anche in questo caso sono previste sanzioni diversificati in ragione dell'ammontare delle imposte fraudolentemente sottratte al

pagamento. Da quanto sopra discende che la condotta penalmente rilevante può, dunque, consistere, rispettivamente: a) nell'alienare simulatamente o nel compiere altri atti fraudolenti sui propri o su altrui beni (quindi un'attività di materiale sottrazione di disponibilità, comma 1, art. 11 D. Lgs. n. 74/2000); b) nell'indicare, nella documentazione presentata ai fini della procedura di transazione fiscale, elementi attivi o passivi diversi da quelli reali (quindi un'attività di falsificazione della consistenza patrimoniale, comma 2).

In riferimento al momento della consumazione del reato, per entrambe le ipotesi si tratta di un reato a consumazione istantanea in quanto, rispettivamente: a) per le ipotesi di cui al 1 comma dell'art. 11 in commento, rileva in tal caso il momento in cui si aliena simulatamente o si compiono altri atti fraudolenti sui propri o su altrui beni; b) per le ipotesi di cui al 2 comma dell'art. 11 in commento, deve guardarsi al momento in cui si presenta la documentazione ai fini della procedura di transazione fiscale corredandola di elementi attivi/passivi diversi da quelli reali.

- **Indebita compensazione (art. 10-quater D. Lgs. n. 74/2000).**

La norma in commento prevede due fattispecie criminose, punendo, tutti i soggetti che non versano le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, per un importo annuo superiore a cinquantamila euro, rispettivamente: a) crediti non spettanti (fattispecie disciplinata dal comma 1, dell'art. in commento); b) crediti inesistenti (fattispecie disciplinata dal comma 2, dell'art. in commento). Per il perfezionamento delle fattispecie criminose in commento non basta il mancato versamento dell'imposta, ma è necessario che lo stessi risulti giustificato dalla compensazione tra i debiti ed i crediti verso l'Erario, allorché i crediti non spettino o non esistano. In questo senso è possibile sottolineare come, per le fattispecie in commento, è la compensazione che rappresenta il *quid pluris* che differenzia il reato dell'art. 10-quater quater del D. Lgs. n. 74/2000 rispetto alle distinte fattispecie di omesso versamento di imposte e/o ritenute. In forza di ciò, la fattispecie di indebita compensazione si consuma, di conseguenza, al momento della presentazione dell'ultimo modello F24 relativo all'anno interessato e non in quello della successiva dichiarazione dei redditi, dal momento che, con l'utilizzo del modello indicato, si perfeziona la condotta ingannevole del contribuente, realizzandosi il mancato versamento per effetto dell'indebita compensazione di crediti in realtà non spettanti in base alla normativa fiscale. Detto altrimenti, la fattispecie ex art. 10 quater del D. Lgs. n. 74/2000 si perfeziona nel momento in cui viene presentato il modello F24 - con "saldo ridotto e/o a zero" - e non invece il termine entro cui presentare la dichiarazione dei redditi.

8.3. IL SISTEMA DEI CONTROLLI.

Alla luce della risk analysis condotta sulla Tao Group in relazione ai reati tributari indicati dal Decreto e sopra elencati, si è provveduto ad analizzare le attività ritenute a rischio e, in particolare, si evidenziano le seguenti attività:

1. Gestione degli accordi di fornitura: definizione delle esigenze di acquisto, selezione dei fornitori, valutazione dei preventivi, verifica dei contratti prima della stipula, definizione delle clausole contrattuali, formulazione di integrazioni/modifiche da apportare al contratto prima della stipula, approvazione dell'ultima versione del contratto, stipula del contratto;
2. Emissione degli ordini di acquisto;
3. Verifica della corrispondenza tra prestazioni/beni acquistati;
4. Gestione delle entrate ed uscite di materiali/merci: inventariazione del materiale, registrazioni di carico e scarico merci da magazzino, gestione degli accessi alle aree riservate allo stoccaggio dei materiali, dismissioni/distruzione dei materiali non più utilizzabili;
5. Gestione anagrafica dei fornitori;
6. Contabilizzazione degli accordi pagati ai fornitori;
7. Gestione delle missioni/trasferte: gestione, controllo e autorizzazione delle note spese; gestione e controllo dei benefit e dei mezzi in dotazione; gestione delle spese di rappresentanza e dei beni in rappresentanza;
8. Gestione delle attività di amministrazione, finanza e controllo;
9. Calcolo delle imposte dirette e indirette, esecuzione dei relativi versamenti, predisposizione e trasmissione delle relative dichiarazioni nei termini di legge;
10. Gestione delle attività che prevedono una interazione diretta con l'Amministrazione Finanziaria;
11. Gestione delle attività amministrativo contabili;
12. Attività finanziaria relativa a: gestione dei flussi finanziari, gestione dei fondi aziendali, impiego di disponibilità liquide, eventuali partecipazioni societarie;
13. Cessione di immobili aziendali o partecipazioni;
14. Gestione delle operazioni straordinarie (comprese: costituzioni di diritti reali di godimento su beni immobili, contratto di affitto di azienda, gestione delle passività nell'ambito di procedure esecutive);
15. Gestione delle operazioni contabili di compensazione;
16. Gestione delle transazioni finanziarie (incassi e pagamenti);
17. Gestione delle risorse finanziarie;
18. Sistema di programmazione, budget e controllo;

19. Gestione del processo di formazione e chiusura del bilancio;
20. Apertura/chiusura di conti correnti: riconciliazione degli estratti conto bancari e delle operazioni di cassa, registrazione degli incassi e dei pagamenti in contabilità generale;
21. Gestione della cassa;
22. Verifica e controllo dell'anagrafica studenti/iscritti ai corsi;
23. Gestione del ciclo di fatturazione passiva;
24. Controlli sulla regolarità delle fatture passive;
25. Registrazione contabile fatture passive e note di credito;
26. Liquidazione delle fatture passive e incassi;
27. Archiviazione della documentazione a supporto delle fatture passive e delle note di credito;
28. Gestione del ciclo di fatturazione attiva;
29. Emissione, contabilizzazione e archiviazione delle fatture attive e delle note di credito;
30. Controlli sulla regolarità delle fatture attive;
31. Registrazione contabile fatture attive e note di credito;
32. Liquidazione delle fatture attive e incassi;
33. Verifica della regolarità dei pagamenti (coincidenza tra destinatari e ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni);
34. Monitoraggio delle fatture da ricevere e in scadenza;
35. Archiviazione della documentazione a supporto delle fatture attive e delle note di credito;
36. Gestione del credito e recupero crediti;
37. Archiviazione dei documenti aziendali, delle scritture contabili, dei bilanci e dei registri fiscali obbligatori;
38. Gestione della fatturazione elettronica;
39. Back-up dell'archivio contabile e relative attività e disaster recovery;
40. Gestione sistemi informatici;
41. Gestione della sicurezza informatica sia a livello fisico che a livello logico: configurazione delle security policy dei firewall ai fini di tutela delle intrusioni esterne, gestione e protezione dei back up dei dati, elaborazione di un sistema di alta affidabilità a tutela del patrimonio informativo, utilizzo di banche dati;
42. Ogni altra area che verrà ritenuta, via via, rilevante.

Eventuali integrazioni delle suddette aree sensibili potranno essere proposte al Consiglio di Amministrazione dell'Organismo di Vigilanza per effetto dell'evoluzione della sua attività e, conseguentemente, di eventuali modifiche dell'attività svolta dalle singole funzioni.

8.4. I PRINCIPI GENERALI DI COMPORTAMENTO

Tutti i soggetti Destinatari coinvolti nelle "aree sensibili" sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal modello e, in particolare, dal Codice Etico E Comportamentale di Tao Group S.r.l.
In generale è fatto di divieto di:
a) porre in essere comportamenti che integrino i Reati Tributari;
b) porre in essere comportamenti che, sebbene non integrino di per sé Reati Tributari, potrebbero potenzialmente diventarlo;
c) porre in essere comportamenti in conflitto di interesse con la società;
d) porre in essere i comportamenti indicati ai precedenti punti sia direttamente, che per interposta persona;
e) richiedere, sollecitare, suggerire a dipendenti e collaboratori comportamenti vietati dal Modello, in particolare, nell'ambito dei suddetti comportamenti è fatto sempre divieto in particolare di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, anche solo in astratto o in via potenziale, possono integrare le fattispecie di reato rientranti tra quelle qui considerate;
- perseguire finalità di evasione di imposte sui redditi o sul valore aggiunto, o di altre imposte in generale;
- introdurre elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto;
- registrare nelle scritture contabili obbligatorie fatture o altri documenti per operazioni inesistenti;
- compiere operazioni simulate oggettivamente o soggettivamente, nonché avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento dell'amministrazione finanziaria;
- occultare o distruggere, in tutto o in parte, le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, con il fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi;
- emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;
- effettuare registrazioni false, incomplete o ingannevoli, ed istituire fondi occulti o non registrati;
- alienare simulatamente o compiere altri atti fraudolenti sui propri beni o su beni altrui, in modo da rendere in tutto o in parte inefficace la procedura di riscossione coattiva

da parte dell'amministrazione finanziaria, al fine di sottrarsi al pagamento delle imposte sui redditi o sul valore aggiunto, ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- utilizzare i fondi e le risorse della società senza formale autorizzazione;
- rappresentare o trasmettere dati falsi, lacunosi, o comunque non rispondenti alla realtà, sulla situazione economica, patrimoniale, finanziaria, fiscale e tributaria della società;
- omettere dati ed informazioni, imposti dalla legge, sulla situazione economica, patrimoniale, finanziaria fiscale e tributaria della società;
- effettuare operazioni straordinarie in violazione delle disposizioni di legge;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento delle attività di controllo da parte dei soci o delle Autorità preposte.

Ai fini dell'attuazione dei comportamenti di cui sopra, sono previste le seguenti condotte:
- tenere un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e regolamentari nonché il rispetto delle procedure aziendali interne, e la massima veridicità, trasparenza e completezza di tutte le informazioni prodotte e gestite, nello svolgimento di tutte le attività in materia tributaria e amministrativo contabili;
- garantire, nell'ambito del sistema di contabilità aziendale, la registrazione di ogni operazione di natura economico/finanziaria nel rispetto dei principi, dei criteri e delle modalità di redazione e tenuta della contabilità dettate dalle normative vigenti;
- garantire, nell'ambito del sistema di contabilità aziendale, la correttezza della rendicontazione delle prestazioni erogate, di quelle ricevute, e dei relativi flussi finanziari;
- assicurare che tutte le operazioni e/o transazioni gestite all'interno della società siano autorizzate, vengano correttamente registrate e siano verificabili, legittime, coerenti e congrue;
- assicurare la massima veridicità, trasparenza e completezza di tutte le informazioni prodotte e gestite nello svolgimento delle attività al fine di garantire la correttezza e l'accuratezza delle informazioni per il calcolo delle imposte e la conseguente presentazione di dichiarazioni e/o documenti fiscali previsti dalla normativa fiscale;
- mantenere una condotta improntata ai principi di correttezza, trasparenza, collaborazione e al rispetto delle norme di legge e regolamentari, allo scopo di fornire un'informazione veritiera e corretta in merito allo svolgimento di ogni operazione o transazione effettuata dalla società;

- documentare in modo chiaro e trasparente tutti i passaggi delle attività svolte;
- osservare scrupolosamente tutte le norme poste dalla legge in materia tributaria e fiscale;
- assicurare la completezza, la veridicità e l'accuratezza della documentazione a supporto di ogni operazione o transazione effettuata dalla società, garantendo la possibilità di poter procedere, per ognuna di esse, in ogni momento, allo svolgimento di controlli volti ad attestare le caratteristiche, le motivazioni ed il flusso informativo;
- predisporre le comunicazioni e le segnalazioni dirette agli organi di controllo nel rispetto dei principi di completezza, integrità, oggettività e trasparenza;
- mettere in atto i necessari controlli per la verifica preventiva delle informazioni disponibili sulle controparti commerciali o istituzionali prima di instaurare qualsiasi tipo di rapporto di affari;
- precludere ad un soggetto non in possesso dei requisiti di integrità, capacità economica e tecnica, di competere per l'ottenimento delle forniture;
- rispettare la normativa prevista dal Codice dei Contratti Pubblici ed informare l'Organismo di Vigilanza nel caso in cui vengano rilevate specifiche anomalie;
- garantire la regolarità dei pagamenti, con riferimento alla piena coincidenza tra i destinatari dei pagamenti stessi e le controparti effettivamente coinvolte nelle transazioni;
- effettuare i pagamenti esclusivamente per le attività contrattualmente formalizzate e/o deliberate dalla società;
- prevedere costante attività formativa, a tutti i destinatari, su quanto previsto dal Codice Etico E Comportamentale e dal Modello organizzativo 231, assicurando diffusione/formazione sulle diverse procedure/protocolli;
- obbligo di consultare l'Organismo di Vigilanza ed il Consiglio di Amministrazione prima di adottare un determinato comportamento, in caso di incertezza sulla liceità / legittimità dello stesso;
- obbligo di comunicare all'Organismo di Vigilanza condotte e/o comportamenti contrari ai principi ed alle norme di legge e/o anomali;
- obbligo di informare l'Organismo di Vigilanza nel caso in cui si riscontrino o si venga a conoscenza di omissioni, falsificazioni o inesattezze nelle registrazioni contabili o negli atti a queste riconducibili.

TAO GROUP S.R.L.
Via G. di Vittorio 216-218
53042 Chianciano Terme (SI)
C.F./P.IVA 01469200529