MODELLO ORGANIZZATIVO

ai sensi del D.Lgs. 231/2001

PARTE SPECIALE 6

Altri Reati

SOMMARIO

1. TIPOLOGIA DI REATI

La presente Parte Speciale si riferisce alle residue fattispecie criminose cui si applica la disciplina della responsabilità amministrativa degli enti e che non rientrano nelle categorie dei reati cui sono dedicate le precedenti Parti Speciali 1, 2, 3, 4 e 5.
Tra questi reati residuali, per alcune fattispecie si è individuato in fase di analisi dei rischi un rischio nullo o marginale, e non vengono dunque qui riportate, rimandandosi alle disposizioni generali del Codice Etico.

1.1 DELITTI CONTRO LA PERSONALITA' INDIVIDUALE

- ✓ *Art. 600 del Codice Penale – Riduzione o mantenimento in schiavitù o in servitù*

Fattispecie
Esercitare su di una persona poteri analoghi a quelli del diritto di proprietà ovvero ridurre o mantenere una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento.
La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittandosi di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Esempio
Sfruttamento del lavoro nero sottopagato e/o di persone non in regola con i permessi di soggiorno.

1.2 DELITTI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA

- ✓ *Art. 377 bis c.p. del Codice Penale – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*

Fattispecie
Il reato in oggetto è integrato dalla condotta di chiunque, mediante violenza, minaccia promessa di denaro o altra utilità, induce la persona che sia chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale a non rendere dichiarazioni ovvero a mentire, pur avendo il dichiarante la facoltà di avvalersi del diritto di non rispondere.

Esempio
Nella ipotesi che vengano indagati il Presidente ed in concorso il Responsabile Amministrativo, il primo, nell'interesse di SAPI o con di questa vantaggio, induce il secondo a non rendere dichiarazioni o a rendere all'autorità giudiziaria mendaci

dichiarazioni favorevoli alla posizione della società, con violenza o minaccia, o con promessa di denaro o altre utilità.

1.3 DELITTI INFORMATICI

- ✓ *Art. 491 bis del Codice Penale* – Falsità in un documento informatico pubblico avente efficacia probatoria
- ✓ *Art.* 615-ter *del Codice Penale* – Accesso abusivo ad un sistema informatico o telematico
- ✓ *Art.* 615-quater *del Codice Penale* – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- ✓ *Art.* 615-quinquies *del Codice Penale* – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- ✓ *Art.* 617-quater *del Codice Penale* – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- ✓ *Art. 617 quinquies del Codice Penale* – Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- ✓ *Art. 635 bis del Codice Penale* – Danneggiamento di informazioni, dati e programmi informatici
- ✓ *Art. 635 ter del Codice Penale* – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- ✓ *Art. 635 quater del Codice Penale* – Danneggiamento di sistemi informatici o telematici
- ✓ *Art.* 635 *quinquies del Codice Penale* – Danneggiamento di sistemi informatici o telematici di pubblica utilità

Fattispecie

Tutte quelle sopra descritte.

Esempio

Modificare fraudolentemente un documento pubblico residente su supporto informatico di qualsiasi carattere per avvantaggiarne la società.
Introdursi in sistemi informatici propri senza autorizzazione allo scopo di conoscerne o variarne i dati nell'interesse della società.
Accedere a postazioni informatiche incustodite, cui sarebbe precluso l'accesso.
Detenere e diffondere in modo abusivo di codici di accesso a sistemi telematici o informatici, credenziali di autenticazione altrui o comunicare a terzi le proprie in cambio di un'utilità per la società.

1.4 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

- ✓ *Art. 513 del Codice Penale – Turbata libertà dell'industria o del commercio*

Fattispecie

Quando chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

Esempio
Diffondere notizie sui prodotti e sulle attività di un concorrente, idonei a determinarne il discredito, oppure appropriandosi di pregi dei prodotti o dell'impresa di un concorrente.

✓ *Art. 515 del Codice Penale - Frode nell'esercizio del commercio*

Fattispecie
Quando chiunque, nell'esercizio di un'attività, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.
Il bene giuridico tutelato si sostanzia nella correttezza degli scambi commerciali, laddove venga inficiata la fiducia che gli operatori ripongono nelle controparti contrattuali.

Esempio
Vendere/promettere prodotti difformi, per qualità, caratteristiche o prestazioni, da quanto dichiarato nelle specifiche pattuite.

✓ *Art. 516 del Codice Penale - Vendita di sostanze alimentari non genuine come genuine*

Fattispecie
Chiunque pone in vendita o mette altrimenti in commercio come genuine sostanze alimentari non genuine.
l presupposto del reato in esame è rappresentato dalla non genuinità degli alimenti, elemento che può essere valutato alla stregua di un criterio naturale ovvero si considerano gli alimenti che sono stati adulterati o contraffatti, ma al contempo la giurisprudenza ha riconosciuto come operante anche un criterio cosiddetto legale, in quanto vengono considerati non genuini anche gli alimenti che non rispettano i requisiti imposti per legge e necessari per la loro qualificazione.

Esempio
Messa in vendita di prodotti alimentari non genuini

✓ *Art. 517 del Codice Penale - Vendita di prodotti industriali con segni mendaci*

Fattispecie
Vendere o mettere altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.

Esempio
Utilizzo indebito dei marchi di certificazione di prodotto.

✓ *Art. 517 ter del Codice Penale - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale*

Fattispecie

Quando chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso.
Il 517 ter mira a tutelare i diritti di proprietà industriale, acquisiti mediante brevetto, registrazione o negli altri modi previsti dalla legge in materia di privativa industriale.

Esempio

Violazione di brevetti esistenti nello sviluppo di nuove tecnologie.

1.5 DELITTI IN MATERIA DI VIOLAZIONE DEI DIRITTI D'AUTORE

- ✓ *art. vari L.633/1941 – Sanzioni penali in materia di diritto d'autore*

Fattispecie

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 ed utilizzo della propria opera.
La disposizione si riferisce anche alla tutela dei software in generale, e delle banche dati. E' infatti prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.
Sono tutelate una serie numerosa di opere dell'ingegno: opere destinate al circuito radiotelevisivo e cinematografico, ma anche opere letterarie, scientifiche o didattiche.

Esempio

Utilizzo e diffusione di software in assenza di apposita licenza nelle attività sociali.

1.6 IMPIEGO DI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO

- ✓ *Art. 22 comma 12 bis D.Lgs. 286/98 – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*

Fattispecie

Azienda che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, nel caso in cui i lavoratori occupati sono (circostanza alternative tra di loro):
- in numero superiore a tre;
- minori in età non lavorativa;
- esposti a situazioni di grave pericolo, con riferimento alle prestazioni da svolgere ed alle condizioni di lavoro.

Esempio

Avere alle proprie dipendenze personale extracomunitario privo di permesso di soggiorno o il cui permesso di soggiorno è scaduto.

1.7 CONTRABBANDO

- ✓ *art. da 282 a 294 D.P.R. 23.01.1973, n.43) – Contrabbando*

Fattispecie
Azienda che introduce nel territorio dello Stato, in violazione delle disposizioni in materia doganale, merci che sono sottoposte ai diritti di confine.

Esempio
Introduzione nel territorio dello Stato, in violazione delle disposizioni in materia doganale, merci che sono sottoposte ai diritti di confine.

2. PRINCIPI DI COMPORTAMENTO

Ai Destinatari del Modello è fatto divieto di:

- porre in essere comportamenti tali da integrare le fattispecie di reato qui considerate;
- porre in essere comportamenti che, sebbene non costituiscano di per sé fattispecie di reato rientranti tra quelle qui considerate, possano potenzialmente diventarle.

I Destinatari del Modello, in particolare gli amministratori, i soggetti in posizione apicale e quanti svolgono la propria attività nelle aree a rischio, devono rispettare le regole e i principi contenuti nei seguenti documenti:

- lo Statuto di SAPI;
- le procedure aziendali, la documentazione, le norme concernenti il sistema amministrativo, contabile, finanziario e di *reporting*, che fanno parte integrante del Sistema di Controllo Interno della Società.

In relazione ai delitti informatici ai Destinatari è fatto espresso divieto di:

- Alterare o rendere false dichiarazioni in documenti informatici pubblici, aventi efficacia probatoria;
- Accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- Accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e o cancellare dati e/o informazioni;
- Detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- Detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- Cedere a terzi codici, parole chiave o altre credenziali di autenticazione tramite le quali sia possibile tentare di accedere o accedere abusivamente al sistema informatico o telematico proprio o altrui, ovvero intercettare comunicazioni tra sistemi informatici diversi, anche di soggetti pubblici;
- Svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- Svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- Installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- Svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

- Svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- Distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
- Inserire presidio relativo a sistema di controllo licenze degli applicativi in uso all'interno dell'ambiente aziendale.
- Utilizzare software provvisti di licenza e installare software sul proprio computer solo in presenza di autorizzazione da parte dell'amministratore di sistema;

In relazione ai delitti contro l'industria ed il commercio ai Destinatari è fatto espresso divieto di:

- Mettere in atto pratiche e accordi in violazione delle leggi sulla concorrenza applicabili nei vari paesi
- Vendere o mettere in circolazione prodotti industriali con nomi, marchi o segni distintivi mendaci, contraffatti o alterati e che possano indurre in inganno l'acquirente sull'origine, provenienza o qualità del prodotto
- Vendere o promettere prodotti diversi da quanto pattuito per qualità, origine, quantità e caratteristiche tecniche
- Sviluppare, fabbricare o adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso;
- Importare file od altre proprietà industriali in qualsiasi forma da precedenti esperienze di lavoro;
- Compiere qualsiasi atto di concorrenza con violenza o minaccia;
- Compiere atti intimidatori al fine di controllare o condizionare attività commerciali o industriali.

In relazione agli altri reati oggetto della presente parte speciale ai Destinatari è fatto espresso obbligo di:

- Assumere personale in regola con i permessi di soggiorno, verificandone anche le scadenze successive, e rispettando le norme in materia previdenziale, verificando il possesso dei requisiti professionali e di onorabilità, nel rispetto della congruità del costo del lavoro e degli orari praticati;
- Evitare il compimento di atti diretti a favorire la permanenza di chi non è in regola con il permesso di soggiorno o destinatario di provvedimenti limitativi della libertà personale;
- Non assegnare incarichi ad imprese di servizi che sfruttano manodopera irregolare o che non prestano attenzione alla congruità del costo del lavoro e degli orari praticati;
- Evitare di spendere monete false ricevute in buona fede
- Rispettare gli adempimenti previsti dal Regolamento UE 2016/679 e dal D.Lgs 196/2003 in materia di trattamento dei dati personali;
- Rendere, davanti alla autorità giudiziaria, dichiarazioni corrispondenti esclusivamente al vero ed astenersi dall'esercitare indebite pressioni di qualsivoglia natura nei confronti di chi è chiamato a rendere dichiarazioni innanzi all'autorità giudiziaria;

- Denunciare eventuali violenze, minacce, o offerte o promesse di denaro o di altra utilità per indurre taluno a non renderle o a renderle mendaci, anche qualora si sia in prima persona chiamati a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale e sia stata posta in essere alcuna delle condotte descritte;
- A chi, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio di:
    - acquistare, vendere o compiere altre operazioni, direttamente o indirettamente, per conto proprio o di terzi, su strumenti finanziari utilizzando le informazioni medesime;
    - comunicare tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
    - raccomandare o indurre altri, sulla base di esse, al compimento di taluna delle operazioni sopra descritte
- Diffondere notizie false o porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

3. ATTIVITA' A RISCHIO E PROTOCOLLI DI PREVENZIONE

I principi di comportamento descritti nel paragrafo precedente, trovano attuazione nelle procedure aziendali, ispirate ai seguenti principi:

- Verificabilità, documentazione, coerenza, congruenza delle operazioni: per cui le attività sensibili devono essere isolate, logicamente definite, e documentate, cosicché siano accertabili anche successivamente le decisioni tratte e le relative responsabilità di autorizzazione, effettuazione, registrazione e verifica;
- Separazione delle responsabilità: per cui nessuno dovrebbe gestire in autonomia un intero processo, dato che la contrapposizione ed il bilanciamento delle responsabilità rappresentano un deterrente rispetto alla commissione di illeciti;
- Documentazione dei controlli: principio secondo il quale deve rimanere evidenza documentale e tracciabilità dei controlli effettuati, anche di supervisione;
- Definizione di poteri autorizzativi e funzionali coerenti con le responsabilità gestionali assegnate, come fattore di prevenzione all'abuso dei poteri stessi, in particolare dal punto di vista economico;
- Comunicazione all'Organismo di Vigilanza delle informazioni rilevanti.

Fermo restando che ogni procedura aziendale, in quanto approvata dall'Amministratore Delegato, è vincolante nella sua interezza, ai fini di una migliore comprensione della loro efficacia preventiva di commissione degli illeciti, nella tabella di seguito riportata vengono evidenziate le correlazioni tra:

- Processi aziendali
- Attività a rischio, con i riferimenti alla codifica delle attività a rischio riportata nell'Analisi dei Rischi
- Procedura, se presenti/previste
- Protocolli di prevenzione declinati all'interno della procedura ai fini della prevenzione degli illeciti

Laddove non presente alcuna correlazione tra attività a rischio ed una procedura specifica o la medesima, pur citata, non sia stata ancora formalmente adottata, fanno testo, ai fini dell'efficacia preventiva, i "protocolli di prevenzione" quivi riportati.

Laddove non sia possibile individuare criteri organizzativi efficaci per prevenire il rischio (esempio: non esistono criteri organizzativi che impediscono di fare corruzione), si rimanda ai principi generali di comportamento ed al Codice Etico.

La codifica delle attività a rischio qui riportate (LETTERA numero) è coerente con quanto riportato nella mappatura dei rischi.

RIF.	PROCESSI	REATI	ATTIVITA' SENSIBILE	RIFERIMENTI DOCUM.	PRINCIPI DI PREVENZIONE
B9	Commerciale	Turbata libertà dell'industria o del commercio	Diffusione di notizie su prodotti o attività di un concorrente		Divieto in Codice Etico e norme di comportamento
B10 D3	Commerciale Produzione	Frode nell'esercizio del commercio Vendita di prodotti industriali con segni mendaci	Produzione e vendita di merci non conformi alle specifiche pattuite	Manuale Qualità e Manuale HACCP e relative procedure di riferimento Procedura PQ CNR 04_Identificazione e tracciabilità dei materiali.	Registri con dettaglio di provenienza e destinazione della merce. Analisi svolte ogni 4 settimane presso laboratorio accreditato. Analisi giornaliera nel laboratorio interno per impurità proteiche residue nel prodotto finito.
B11	Commerciale	Vendita di sostanze alimentari non genuine come genuine	Introduzione in commercio di prodotti alimentari non genuini	Manuale Qualità e Manuale HACCP e relative procedure di riferimento	
A3	R&D	Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale	Sviluppo e utilizzo di nuove tecnologie		Divieto di sviluppo di nuovi prodotti e tecnologie in violazione di brevetti esistenti in Codice Etico e norme di comportamento.
C14	Approvvigionamento	Contrabbando	Importazione di merci dall'estero		Utilizzo di spedizionieri terzi specializzati
C10 E3	Approvvigionamenti Infrastrutture	Delitti contro la personalità individuale - Riduzione in schiavitù	Appalti di servizi o di lavorazioni esterne ad imprese che sfruttano manodopera irregolare	Procedura P_S_G_01 - Gestione delle attività in appalto.	Ottenimento di DUVRI, DURC, elenco dei lavoratori ed estratto LUL e documentazione che accerti la regolarità del soggetto. Congruità dei prezzi applicati, determinati richiedendo più preventivi oppure sulla base dei tempi e costi standard del settore. Clausola codice etico nei contratti. Divieto di subappalto salvo autorizzazione.
F7	Gestione Risorse Umane	Delitti contro la personalità individuale - Sfruttamento del lavoro	Assunzione e gestione del personale		Le assunzioni sono effettuate tramite consulente esterno e nel rispetto del CCNL. Divieto in Codice Etico e norme di comportamento

RIF.	PROCESSI	REATI	ATTIVITA' SENSIBILE	RIFERIMENTI DOCUM.	PRINCIPI DI PREVENZIONE
F8	Gestione Risorse Umane	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Assunzione e gestione del personale	Procedura PO_P_G_01 Ricerca e selezione del personale.	Richiesta permesso di soggiorno in fase di assunzione. Scadenziario verifica validità permessi di soggiorno.
L14	Legale e Societario	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Cause giudiziarie		Correttivi generali previsti per evitare la corruzione Divieto in Codice Etico e norme di comportamento. Notifica ad OdV di cause giudiziarie.
M1	Sistemi informativi	Falsità in un documento informatico pubblico avente efficacia probatoria	Redazione di atti pubblici residenti su supporto informatico		Codice Etico e norme di comportamento
M2 M3 M4	Sistemi informativi	Delitti informatici vari	Utilizzo della rete aziendale e di internet		Documentazione Privacy ai sensi del Reg. UE 2016/679. Adempimenti privacy sulle credenziali di autenticazione Divieto in Codice Etico e norme di comportamento. Estendere Codice Etico a consulenti informatici.
M5	Sistemi informativi	Violazione diritti d'autore	Utilizzo di software sprovvisti di licenza	Regolamento aziendale locale per uso degli strumenti elettronici e informatici	Mappatura periodica e documentata dei software installati.

4. COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA

È fatto obbligo ai Destinatari di comunicare all'Organismo di Vigilanza i seguenti eventi:

- Cause giudiziarie ed arbitrati;
- Sanzioni in materia di trattamento dei dati personali;
- Notizie di comportamenti a rischio di reato ai sensi del D.Lgs. 231/2001, in via diretta o indiretta.