18. SPECIFICI PROTOCOLLI RIFERITI AI REATI PRESUPPOSTO

18.1. PREMESSA

Nel presente capitolo si affronta no gli specifici protocolli riferiti ai reati presupposto nella maniera più semplice e schamatica possibile, ben sapendo che sia i "protocolli" proposti sia gli altri che andremo a illustrare nelle eventuali prossime edizioni possono essere presentati in maniera incompleta se riferiti all'azienda a cui devono essere applicati.
Sarà compito dell'organo di governance preposto alla loro stsura dal CdA ad adattarli alle esigenze specifiche.
Nel presente capitolo si riportano i protocolli al fine di prevenire la commissione dei reati presupposto ex D.Lgs. 231/2001[1].
Si ricorda qui che il decreto 8 giugno 2001 numero 231 all'art 6 comma 2 lettera b prescrive quanto segue: "*b) prevedere* ***specifici protocolli*** *diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*".
Si ricorda che con il termine protocollo e/o procedura si intende "*un insieme di principi, situazioni, meccanismi organizzativi e operativi di comportamento che é funzionale alla gestione del rischio-reato, nel senso che la sua corretta applicazione, anche in combinazione con altri protocolli e/o procedure, é tale da prevenire la commissione del reato da cui sorge la responsabilità ex d.lgs. 231/2001"*.

Si riportano qui di seguito i reati presupposto elencati nel D.Lgs. 231/2001[2]:
I – Reati commessi nei rapporti con la pubblica amministrazione.
II – Delitti informatici e trattamento illecito di dati - *art. 24-bis, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 48/2008)*
III – Delitti di criminalità organizzata - *art. 24-ter, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 94/2009)*
IV – Concussione, induzione indebita a dare o promettere altra utilità e corruzione *(art. 25, d.lgs. n. 231/2001) (articolo modificato dalla L. n. 190/2012)*
V – Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento - *art. 25-bis, D.Lgs. n. 231/2001 (articolo aggiunto dal d.l. n. 350/2001, convertito con modificazioni dalla l. n. 409/2001 ed ulteriormente modificato dalla l. n. 99/2009)*
VI – Delitti contro l'industria e il commercio - *art. 25-bis.1, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 99/2009)*

[1] Il lettore troverà il dettaglio nel CD (14).
[2] I reati e gli illeciti qui considerati sono oggetto di costante aggiornamento legislativo. Pertanto, il presente testo proposto dei protocolli e procedure qui proposto è suscettibile di subire, in futuro, integrazioni e variazioni, anche significative, al fine di garantirne la conformità e l'aderenza alla normativa vigente.

18. Specifici protocolli riferiti ai reati presupposto

18.1. Premessa

VII – Reati societari - *art. 25-ter, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 61/2002 e successivamente modificato con l. n. 262/2005, l. n. 190/2012 e da ultimo con l. n. 69/2015)*
VIII – Delitti con finalità di terrorismo o di eversione dell'ordine democratico - *art. 25-quater, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 7/2003)*
IX – Pratiche di mutilazione degli organi genitali femminili - *art. 25-quater.1, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 7/2006)*
X – Delitti contro la personalità individuale - a*rt. 25-quinquies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 228/2003 e successivamente modificato con l. n. 38/2006, d. lgs. n. 39/2014 e l. n. 199/2016)*
XI – Abusi di mercato - *art. 25-sexies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 62/2005)*
XII – Omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro - *art. 25-septies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 123/2007 e successivamente modificato con d.lgs. n. 81/2008)*
XIII – Ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita, nonchè autoriciclaggio - *art. 25-octies, d.lgs. n. 231/2001 (articolo aggiunto dal d. lgs. n. 231/2007 e modificato dalla l. n. 186/2014)*
XIV – Delitti in materia di violazione del diritto d'autore - *art. 25-novies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 99/2009, successivamente modificato con l. n. 116/2009 e con d.lgs. n. 121/2011)*
XV – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria - *art. 25-decies, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 121/2011)*
XVI – Reati ambientali - *art. 25-undecies, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 121/2011, modificato dalla l. n. 68/2015)*
XVII – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare - *art. 25-duodecies, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 109/2012)*
XVIII – Razzismo e xenofobia (art. 25-terdecies, d.lgs. n. 231/2001) [articolo aggiunto dalla legge 20 novembre 2017 n. 167]. *Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale (art. 3, comma 3-bis della legge 654/1975)*
XIX – Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25 - *quaterdecies* D.Lgs. n. 231/2001 - Legge n. 39/2019)
XX – Reati tributari (Art. 25 - *quinquiesdecies*, D.Lgs. n. 231/2001 - Legge n. 157/2019)
XXI – Delitto di contrabbando *(*art. 25-*sexiesdecies*, *D.Lgs. n. 231/2001 - D.Lgs. 14 luglio 2020, n. 75 attuativo della Direttiva (UE) 2017/1371)*
XXII – Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato - *art. 12, l. n. 9/2013 (costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva)*
XXIII – Reati transnazionali (l. n. 146/2006) [costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

18.1.1 Protocolli riferiti ad alcuni reati presupposto

La governance aziendale ha il compito di redigere dei protocolli e procedure adeguati all'azienda che gestiscono e nel seguito del loro incarico di aggiornali e ciò in riferimento a quanto richiesto (D. Lgs. 231/2001, art. 6 comma 2 b): prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire).

L'estensore del MOGC e L'Organismo di Vigilanza hanno il compito di controllare i protocolli e procedure in modo che essi siano adeguati all'azienda in cui operano e nel seguito del loro incarico di aggiornali.
Gli autori propongono qui alcuni dei protocolli o procedure che possono essere applicate e adattate con le opportune integrazioni a qualsiasi società od ente[3].
Si ricorda qui che gli specifici protocolli, redatti da un organo o professionista nominato dal CdA e da questo incaricato, hanno carattere interno all'azienda e sono riservati agli organi che li devono applicare.
Essi possono essere integrati da richiami alla normativa ed alle leggi vigenti.
I reati presupposto cui i curatori della presente edizione si sono concentrati sono[4]:

- **I** – Reati commessi nei rapporti con la pubblica amministrazione. *Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico – art. 24, D.Lgs. n. 231/2001* (articolo modificato dalla L. 161/2017).
- **II** – Delitti informatici e trattamento illecito di dati - *art. 24-bis, D.Lgs. n. 231/2001 (articolo aggiunto dalla L. n. 48/2008 modificato dal D.Lgs. n. 7 e 8/2016)*
- **III** – Delitti di criminalità organizzata - *art. 24-ter, D.Lgs. n. 231/2001 (articolo aggiunto dalla L. n. 94/200e modificato dalla L. 69/2015)*
- **V** – Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento - *art. 25-bis, d.lgs. n. 231/2001 (articolo aggiunto dal d.l. n. 350/2001, convertito con modificazioni dalla l. n. 409/2001 ed ulteriormente modificato dalla l. n. 99/2009).*
- **VI** – delitti contro l'industria e il commercio - *art. 25-bis.1, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 99/2009).*
- **VII** – reati societari - *art. 25-ter, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 61/2002 e successivamente modificato con l. n. 262/2005, l. n. 190/2012 e da ultimo con l. n. 69/2015).*

---

[3] Il metodo ed i protocolli qui proposti vogliono dare una soluzione più completa possibile. Il professionista e/o manager che voglia redigere e presentare agli organi di governance societari dei specifici protocolli può scegliere una delle due alternative:
a) seguire i protocolli qui proposti adattandoli alle specifiche necessità dell'azienda a cui andranno applicati e convenientemente migliorarli.;
b) creare *motu proprio* dei protocolli *ex novo*.
Il lavoro che viene qui proposto segue la prima via; cioè viene presentato al lettore un percorso professionale dettagliato; il professionista (consulente economico o legale) o il Dirigente Aziendale incaricato di redigere le procedure e i specifici protocolli pretesi dal decreto 231/2001 esaminerà in senso critico quanto qui presentato, l'esperienza e la pratica professionale maturata gli permetteranno di adeguare ed adattare ogni singolo strumento alla situazione aziendale specifica.

[4] Si è deciso di dedicare capitoli specifici al tema della salute e sicurezza sul lavoro ed ambiente in quanto materie in cui sono coinvolte gran parte delle aziende e che, dalle notizie note a tutti e dalle statistiche nazionali, i reati ascritti a dette categorie risultano essere quelli che implicano delle responsabilità veramente impegnative per le aziende con conseguenze a volte disastrose. Nei capitoli 20 e 21 si propongono delle appropriate check list riferite ai reati presupposto in materia sicurezza sul lavoro ed ambiente.

- **X** – delitti contro la personalità individuale - a*rt. 25-quinquies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 228/2003 e successivamente modificato con l. n. 38/2006, d. lgs. n. 39/2014 e l. n. 199/2016).*
- **XII** – Omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro - *art. 25-septies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 123/2007 e successivamente modificato con d.lgs. n. 81/2008).* Esaminato nel Capitolo 20.
- **XIII** – Ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita, nonchè autoriciclaggio - *art. 25-octies, D.Lgs. n. 231/2001 (articolo aggiunto dal D. Lgs. n. 231/2007 e modificato dalla L. n. 186/2014)*
- **XIV** – Delitti in materia di violazione del diritto d'autore - *art. 25-novies, d.lgs. n. 231/2001 (articolo aggiunto dalla l. n. 99/2009, successivamente modificato con l. n. 116/2009 e con d.lgs. n. 121/2011).*
- **XV** – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria - *art. 25-decies, D.Lgs. n. 231/2001 (articolo aggiunto dal D.Lgs. n. 121/2011)*
- **XVI** – Reati ambientali - *art. 25-undecies, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 121/2011, modificato dalla l. n. 68/2015).* Esaminato nel Capitolo 21.
- **XVII** – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare - *art. 25-duodecies, d.lgs. n. 231/2001 (articolo aggiunto dal d.lgs. n. 109/2012).*
- **XX** – Reati tributari (Art. 25-quinquiesdecies, D. Lgsl. n. 231/2001)

18.2. PROTOCOLLO PER REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (I)

1. Reati presupposto.
2. Caratteristiche generali dei reati contro la Pubblica Amministrazione.
3. Individuazione delle aree di attività a rischio.
4. Destinatari.
5. Regole di carattere generale.
6. Documenti diffusi tra gli organi Sociali dell'azienda.
7. Protocolli specifici.
8. Flussi informativi e attività dell'Organismo di Vigilanza (OdV).
9. Linee guida di Confindustria del marzo 2014 (non definite nel documento).

Superiore immediato	
Responsabile della regola normativa	

18.2.1 Reati presupposto

Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello

Stato o di un ente pubblico – *art. 24, D.Lgs. n. 231/2001*(articolo modificato dalla L. 161/2017).

18.2.2 Caratteristiche generali dei reati contro la Pubblica Amministrazione

Ai sensi dell'art. 6 del Decreto, sono state individuate dalla Società le attività sensibili nell'ambito delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del Decreto. Il processo di individuazione di dette attività ha valutato i profili potenziali di rischio di reato in relazione ai rapporti che la Società intrattiene con la Pubblica Amministrazione. Si osserva che ai fini del Modello appartengono alla Pubblica Amministrazione tutti quei soggetti, pubblici o privati, che svolgono una "funzione pubblica" o un "pubblico servizio" ai sensi degli artt. 357 e 358 del Codice Penale.
Per **funzione pubblica** si intende l'esercizio delle attività, disciplinate da norme di diritto pubblico, attinenti alla funzione legislativa, amministrativa e giudiziaria. La funzione pubblica è caratterizzata dall'esercizio del potere autoritativo e del potere certificativo. Colui che "esercita una pubblica funzione legislativa, giudiziaria o amministrativa" è qualificato, ai sensi dell'art. 357 c.p., quale "pubblico ufficiale".
Per **pubblico servizio** si intende, invece, l'esercizio delle attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'Autorità Pubblica o l'esercizio delle attività volte a garantire i diritti fondamentali della persona, quali quello alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione, etc. Il pubblico servizio è un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri autoritativi e certificativi. Colui che "a qualunque titolo presta un pubblico servizio" è qualificato, ai sensi dell'art. 358 c.p., quale "persona incaricata di un pubblico servizio".

18.2.3 Individuazione delle aree di attività a rischio

La mappatura delle attività a rischio in relazione ai reati di cui agli artt. 24 e 25 del Decreto ha consentito di individuare, non solo le attività c.d. sensibili in senso stretto ma anche una serie di attività strumentali per le quali, quindi, sono stati individuati specifici principi di comportamento e misure di prevenzione e controllo.
Con **attività sensibili** si intendono quelle attività che presentano rischi diretti di rilevanza penale in relazione ai Reati Presupposto individuati dal Decreto.
Le **attività strumentali** sono le attività che, pur non presentando rischi diretti di rilevanza penale, se combinate con le attività direttamente sensibili, possono supportare la realizzazione del reato e sono quindi funzionali alla condotta illecita.
Ai sensi dell'art. 6 del Decreto, sono state individuate dalla Società le attività sensibili nell'ambito delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del Decreto:

– **i rapporti con uffici, organi, funzioni, Enti della P.A**., nell'ambito di procedimenti amministrativi, nonché nell'ambito di attività di ispezione e controllo svolte dagli apparati pubblici sull'attività aziendale; si tratta di attività che possono

identificarsi in singole Operazioni a Rischio, definite nel tempo ed individuabili separatamente;
- **i rapporti con la P.A. collegati alla specifica attività aziendale**, e relativi principalmente alle verifiche e autorizzazioni da parte della P.A., necessarie all'azienda per lo svolgimento della specifica attività aziendale;
- i rapporti con la P.A. collegati alla richiesta e fruizione di finanziamenti o benefici erogati dallo Stato, la Comunità Europea e altri Enti pubblici locali, nazionali o comunitari.

Particolare attenzione va prestata nelle seguenti attività a rischio:
- **i rapporti con i vari uffici della pubblica amministrazione per l'ottenimento di permessi, concessioni, autorizzazioni** o altri provvedimenti abilitativi; in particolare oltre alle autorizzazioni o licenze generalmente correlate agli interventi sulle proprietà immobiliari aziendali e in materia ambientale, assumono rilievo specifico la necessità di ottenere autorizzazioni al trasporto di sostanze pericolose o rifiuti in regime di ADR per una parte delle materie prime, semilavorate o residue trattate dall'azienda nel proprio ciclo produttivo;
- i rapporti con i servizi della pubblica amministrazione di **ispezione e vigilanza** (ambientale, amministrativa, fiscale, previdenziale, sanitaria etc.);
- i rapporti con l'amministrazione della giustizia nell'ambito o in occasione di **procedimenti giudiziari** di natura civile, amministrativa, tributaria e penale, che coinvolgano la Società;
- l'avvio e la gestione di procedure per l'ottenimento di **erogazioni o contributi** da parte delle PP.AA. italiane o comunitarie e la gestione dei fondi eventualmente erogati;
- la **produzione di documentazione** alla P.A., anche attraverso i mezzi informatici;
- gestione dei rapporti con l'amministrazione della giustizia nell'ambito o in occasione di procedimenti giudiziari di natura giuslavoristica che coinvolgano la Società;
- ricerca e sviluppo di nuovi prodotti o soluzioni tecniche (quali ad es. macchinari aziendali sviluppati internamente e destinati ad essere utilizzati in aziende terze);
- la trasmissione di dati in via informatica a soggetti pubblici, ad esempio all'Agenzia delle Entrate o agli Enti previdenziali o assicurativi, o comunque l'elaborazione e la trasmissione di documenti aventi efficacia probatoria.

Nel corso della mappatura delle attività sensibili per i reati contro la Pubblica Amministrazione sono state inoltre evidenziate le seguenti attività strumentali, il cui svolgimento potrebbe, potenzialmente, rappresentare un mezzo per la commissione di un Reato Presupposto contro la Pubblica Amministrazione (ad es. creando fondi da utilizzare per finalità corruttive):
- la selezione ed assunzione di personale dipendente;
- gestione delle risorse finanziarie della Società (incassi e pagamenti);
- gestione delle carte di credito corporate, note spese e anticipi;
- gestione di sponsorizzazioni;
- gestione di dotazioni e utilità aziendali (es. pc, autovetture etc.);
- gestione dei rapporti con i fornitori.

18.2.4 Destinatari

Destinatari della presente Parte Speciale sono in primo luogo gli Amministratori, i Dirigenti preposti alla redazione gestione dei contatti, i Sindaci e gli altri soggetti di *Al & El Spa* che si trovano in posizione apicale nonché i soggetti sottoposti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito denominati "Destinatari".
Per quanto concerne gli Amministratori e tutti coloro che svolgono funzioni di direzione dell'ente, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 c.c., infatti, dei reati societari previsti dal Codice Civile risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo i poteri tipici inerenti alla qualifica o alla funzione.
Obiettivo è che tutti i destinatari, come sopra individuati, siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla Società, al fine di prevenire ed impedire il verificarsi dei reati previsti in tale ambito.

18.2.5 Regole di carattere generale

Tutti i Destinatari del Modello, come individuati dalla Parte Generale, adottano regole di comportamento conformi ai principi di seguito elencati, nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili e strumentali indicate nel paragrafo precedente, al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione rilevanti per la Società e previsti dal Decreto.
In generale, si stabiliscono i seguenti principi di comportamento per le attività sensibili relative ai reati di cui agli artt. 24 e 25 del Decreto.
È fatto divieto a tutti i Destinatari del Modello di:
- intrattenere rapporti con la Pubblica Amministrazione, in rappresentanza o per conto della Società, in mancanza di apposita delega o procura della Società stessa;
- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, anche acquisite al di fuori della propria realtà professionale, al fine di influenzarne le decisioni, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del settore, erogazione di contributi/finanziamenti pubblici e/o simili informazioni;
- offrire denaro o altra utilità a Pubblici Ufficiali o incaricati di Pubblico Servizio o organi o funzionari dell'Autorità Giudiziaria, inclusi i familiari degli stessi, al fine di influenzarne la discrezionalità, l'indipendenza di giudizio o per indurli ad assicurare un qualsiasi vantaggio alla Società, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del settore e/o erogazione di contributi/finanziamenti pubblici e/o simili informazioni;
- riconoscere, in favore di fornitori o collaboratori esterni, o loro familiari, che operino nei confronti della Pubblica Amministrazione in nome e per conto della

Società, compensi indebiti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione o dazione di denaro o altra utilità a un pubblico funzionario dell'Autorità Giudiziaria, o suoi familiari, nel caso in cui la Società sia parte di un procedimento giudiziario;
- conferire incarichi professionali, dare o promettere doni, danaro, o altri vantaggi a chi effettua gli accertamenti e le ispezioni, autorità pubbliche ovvero ad organi dell'Autorità Giudiziaria;
- ricorrere a forme di contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze, pubblicità, configurino, invece, forme di doni o regalie verso pubblici funzionari, loro familiari, enti e autorità pubbliche; presentare dichiarazioni, comunicazioni o documenti contenenti informazioni non veritiere, fuorvianti o parziali alla Pubblica Amministrazione, ovvero omettere informazioni, al fine di ottenere provvedimenti favorevoli dalla Pubblica Amministrazione (ad es. per ottenere il rilascio di concessioni o autorizzazioni, finanziamenti pubblici);
- destinare a finalità diverse da quelle per le quali sono stati concessi contributi, sovvenzioni o finanziamenti o altra erogazione dello stesso tipo ottenuti dallo Stato o da altro ente pubblico o dall'Unione Europea.

In particolare, inoltre:
- le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione e realizzazione, nonché di controllo;
- l'Azienda regola la propria politica retributiva e di carriera tenendo in debita considerazione la correttezza e legalità dei comportamenti, penalizzando ogni comportamento che tenda al raggiungimento di obiettivi a discapito del rispetto delle regole aziendali o legali;
- qualsiasi rapporto con funzionari pubblici è corretto, formale ed attento alle molteplici implicazioni che da esso possono derivare;
- l'assunzione di personale dipendente avviene secondo criteri oggettivi di individuazione delle necessità aziendali e delle corrispondenti capacità e titoli individuali, con processo condiviso da più funzioni aziendali che contribuiscono alla scelta dei candidati nel rispetto dei predetti criteri;
- l'opportunità di accesso a finanziamenti e contributi pubblici è individuata sulla base della effettiva presenza di tutti requisiti legali richiesti; una volta ottenuto il beneficio, lo stesso è utilizzato esclusivamente nell'ambito e per le finalità individuati dal provvedimento di erogazione, nel rispetto di tutte le modalità attuative previste, fornendo alla P.A. competente una rendicontazione trasparente, completa e veritiera delle attività finanziate svolte;
- le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella Parte Generale del presente Modello.

18.2.6 Documenti diffusi tra gli organi Sociali dell'azienda

In linea con i principi generali sopra riportati, la Società si è dotata ed ha debitamente formalizzato e divulgato al proprio interno i seguenti documenti:
- Organigramma generale e funzionale suddiviso per (*specificare*).
- Comunicazioni interne di variazione dell'assetto organizzativo e di attribuzione di nuovi compiti e responsabilità ad opera della Direzione Risorse Umane.
- Sistema disciplinare di cui al CCNL ed al MOGC.
- Regole civilistiche e GAAP per la formazione del bilancio e tenuta della contabilità.
- Codice Etico.

18.2.7 Protocolli specifici

In particolare, oltre alle regole generali che sono applicate in via generale in relazione a tutte le attività sensibili individuabili ai sensi del decreto e che devono informare i presenti principi speciali oltreché i relativi protocolli e procedure aziendali, sono stati identificati, per ciascuna differente attività sensibile, i seguenti principi specifici di comportamento, quali misure di prevenzione e controllo, che saranno meglio specificati, ove del caso, negli ulteriori protocolli e procedure aziendali richiamate.
L'Azienda ha sviluppato ed è dotata dei seguenti protocolli:
- Codice Etico;
- Organigramma funzionale e Struttura Organizzativa Aziendale;
- comunicazioni aziendali relative ai compiti e le responsabilità a seguito di variazioni o di integrazioni organizzative;
- Manuale Aziendale integrato del Sistema Qualità, Sicurezza e Ambiente, che disciplina Procedure, Istruzioni Operative, Linee Guida e Schede operative, alle quali si rinvia;
- SGA certificato conforme alla norma ISO 14001;
- SGQ certificato conforme alla norma ISO 9001;
- protocollo sulle Relazioni con la Pubblica Amministrazione[5];
- protocollo sulla formale attribuzione di deleghe e poteri di utilizzazione della firma sociale*;
- protocollo sulla richiesta e gestione finanziamenti e benefici pubblici*;
- procedura specifica per la gestione dei finanziamenti pubblici finalizzati alla formazione del personale*;
- procedure per l'assunzione del personale dipendente

Si riporta di seguito una breve descrizione dei protocolli specifici richiesti:
- **Congruità del prezzo**: il prezzo dell'accordo deve essere ispirato a valori di mercato e / o commisurato alla natura e alle caratteristiche dell'operazione.
- **Clausola 231:** negli accordi con fornitori e partner deve essere inserita una clausola contrattuale secondo la quale la controparte si impegna ad operare

[5] Cap. 17.

rispettando i principi del D.lgs. 231, prevedendo in caso contrario la possibilità per la società di risolvere il contratto e / o applicare una sanzione per le violazioni rilevate.

- **Modalità di pagamento definite**: devono essere chiaramente identificate e formalizzate le modalità di pagamento aziendali e le regole di utilizzo degli strumenti di pagamento (carte di credito, bonifici,). In particolare, si stabilisce il divieto dell'utilizzo di contanti o di strumenti analoghi.
- **Modalità di sourcing definite**: la scelta della modalità di approvvigionamento da adottare (pubblicazione del bando, fornitore unico, utilizzo di vendor list qualificate) deve essere formalizzata ed autorizzata ad un adeguato livello gerarchico e rispettare la normativa in materia; in particolare si stabilisce quanto segue:
  - il ricorso al fornitore unico deve essere ristretto ad una casistica limitata e chiaramente individuata, adeguatamente motivato e documentato, sottoposto a idonei sistemi di controllo e sistemi autorizzativi ad un adeguato livello gerarchico;
  - il ricorso ad approvvigionamenti in condizioni di urgenza richiede la definizione chiara delle condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura e devono essere definiti adeguati strumenti autorizzativi e di monitoraggio (report sottoposti ad adeguato livello gerarchico);
  - le principali fasi della gara (dall'apertura delle offerte fino all'aggiudicazione del contratto) devono essere tracciate e vi devono partecipare soggetti con interessi contrapposti (sia approvvigionamenti che unità richiedente); deve inoltre esistere un modello di valutazione delle offerte (tecniche / economiche) improntato alla trasparenza e alla maggiore limitazione possibile di criteri di soggettività.
- **Valutazione controparte in fase preliminare e in fase di contratto**: prima dell'instaurazione di rapporti contrattuali con terzi, devono essere effettuate le opportune valutazioni sulla controparte con riferimento ai seguenti aspetti:
  - *professionalità*, coerentemente alla natura e all'oggetto dell'accordo,
  - *affidabilità etica*, con riferimento all'eventuale esposizione della controparte a reati di natura 231.
  - nel corso del rapporto contrattuale devono essere poste in essere specifiche attività di controllo che assicurino che la controparte stia operando nel rispetto dei principi 231 e secondo le regole dell'accordo definito.
- **Evidenza svolgimento contenzioso**: devono essere tracciate le fasi principali relative allo svolgimento di un contenzioso di natura giudiziale o stragiudiziale, indicando: oggetto di contenzioso, controparte coinvolta, funzioni aziendali interne, eventuali collaboratori esterni incaricati, accordo finale.
- **Monitoraggio sull'andamento dell'operazione**: devono essere poste in essere specifiche attività di controllo sull'andamento dell'operazione rispetto agli obiettivi aziendali e alle motivazioni che hanno fatto nascere l'operazione.

- **Criteri di valutazione propedeutica dell'operazione**: devono essere definiti i criteri di valutazione delle operazioni societarie, al fine di garantirne la coerenza con le strategie e gli obiettivi aziendali.
- **Monitoraggio periodico su pagamenti esteri**: devono essere svolte specifiche attività di controllo sui pagamenti effettuati in paesi esteri volte a verificare che il pagamento sia coerente con le attività e gli accordi aziendali stipulati, che sia stato correttamente autorizzato e che sia indirizzato al corretto beneficiario, in linea con quanto indicato nell'accordo.
- **Monitoraggio su software, programmi e applicazioni informatiche**: devono essere definite le regole per l'utilizzo degli strumenti informatici aziendali e le attività di controllo su software, programmi, applicazioni informatiche installate su tali dispositivi, al fine di verificare che non vengano scaricate applicazioni potenzialmente utili alla commissione di attività illecite e / o contrarie alle disposizioni aziendali definite (es. manomettere il sistema informatico di terzi, accedere impropriamente al sistema dei pagamenti interno per finanziare la commissione di reati 231).
- **Controllo sicurezza su accesso a sistemi**: devono essere definiti criteri e regole di autorizzazione per l'accesso ai sistemi informatici aziendali; tali accessi devono essere costantemente monitorati in termini di utenti che vi accedono e attività consentite.
- Devono essere inoltre implementate **adeguate misure di sicurezza** che impediscano l'accesso al sistema informativo del Gruppo da parte di terzi non autorizzati (dotazione di firewall).
- **Monitoraggio su tipologie di fatturazione che potrebbero contenere eventuali anomalie:** devono poste in essere specifiche attività di controllo di primo e secondo livello sul processo di fatturazione, al fine di identificare eventuali anomalie.

18.2.8 Flussi informativi e attività dell'Organismo di Vigilanza (OdV)

Per ciascun processo sensibile, il Responsabile Interno deve:
- tenere a disposizione dell'OdV ogni eventuale documentazione di supporto;
- segnalare all'OdV e richiedere la sua assistenza per ogni situazione che si ritenga non conforme alle regole aziendali in materia o laddove si evidenzi comunque una situazione di anomalia.

L'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, delle fasi di ciascun processo che implichi un contatto con la P.A., evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.
L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello, fermo restando il dovere di osservare il divieto di comunicare e/o diffondere le

informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste da forze di polizia, dall'autorità giudiziaria, da organismi di sicurezza o da altri soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione di reato.

18.2.9 Linee guida di Confindustria del marzo 2014[6]

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

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

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

Partecipazione ad una gara indetta da un soggetto pubblico, ovvero presentazione di istanze alla P.A. al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc) di interesse aziendale (ad es. mediante la produzione di documenti falsi attestanti l'esistenza di condizioni e/o requisiti essenziali).	Specifiche previsioni nel sistema aziendale di programmazione e di controllo. Puntuali attività di controllo gerarchico (incluso sistema
Attività aziendali che prevedano l'accesso nei confronti di sistemi informativi gestiti dalla PA, quali, a titolo esemplificativo: - la partecipazione a procedure di gara che prevedono comunque una gestione informatica (ad es. mediante l'alterazione di registri informatici della PA per far risultare esistenti condizioni essenziali per la partecipazione: iscrizione in albi, ecc.);	Sistema di controlli interno all'azienda che, ai fini del corretto e legittimo accesso ai Sistemi informativi della PA, preveda: - un adeguato riscontro delle *password* di abilitazione per l'accesso ai Sistemi Informativi della PA possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche funzioni/strutture aziendali;

[6] Scheda tratta da Linee Guida Confindustria 2014.

- la presentazione in via informatica alla P.A. di istanze e documentazione di supporto, al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc) di interesse aziendale (ad es. laddove contenenti attestazioni/certificazioni non veritiere in merito all'esistenza di condizioni e/o requisiti essenziali); - i rapporti con soggetti della P.A. competenti in materia fiscale o previdenziale in relazione alla ipotesi di modifica in via informatica dei dati (es. fiscali e/o previdenziali) di interesse dell'azienda (es. modelli 770), già trasmessi alla P.A	- la puntuale verifica dell'osservanza, da parte dei dipendenti medesimi, di ulteriori misure di sicurezza adottate dalla società; - il rispetto della normativa sulla *privacy*. Questi meccanismi assumono maggiore pregnanza per quelle società o enti che, sulla base di un rapporto di appalto/concessione con una PA o in qualità di società miste partecipate da un'Amministrazione/Ente locale e da un privato imprenditore, si assumono l'incarico di realizzare, sviluppare e gestire un Sistema Informativo pubblico o un Sistema Informativo di interesse pubblico
Le aree maggiormente a rischio sono relative a: - settore delle attività finanziarie; - investimenti ambientali; - investimenti di produzione; - ricerca ed innovazione tecnologica.	Specifica previsione del Codice Etico e diffusione di quest'ultimo tra tutti i dipendenti. Programma di informazione/formazione periodica del dipendente. Responsabilizzazione esplicita, riportata in ordine di servizio e nel contesto delle relative procedure aziendali, delle funzioni competenti alla predisposizione dei progetti e delle relative istanze. Separazione funzionale fra chi gestisce le attività di realizzazione e chi presenta la documentazione di avanzamento.
	Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto). Coerenza delle procure verso l'esterno con il sistema delle deleghe. Esclusione esplicita, nel sistema delle procure, della "richiesta di denaro o altra utilità a terzi". Puntuali attività di controllo gerarchico, previste altresì in sede di Ordine di servizio delle Funzioni competenti che partecipano al processo di acquisizione di beni e servizi per la società.

Partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego. In tale contesto, assumono particolare rilevanza i seguenti ambiti di operatività: - formazione; - ricerca ed innovazione tecnologica; - investimenti ambientali; - gestione delle attività finanziarie; - investimenti di produzione.	Controlli di completezza e correttezza della documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto). Verifiche incrociate di coerenza tra la funzione richiedente l'erogazione pubblica e la funzione designata a gestire le risorse per la realizzazione dell'iniziativa dichiarata. Monitoraggio sull'avanzamento del progetto realizzativo (a seguito dell'ottenimento del contributo pubblico) e sul relativo *reporting* alla PA, con evidenza e gestione delle eventuali anomalie. Controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati

Emissione Data	data	Edizione	Natura della modifica	Preparato da	Rivisto da	Approvato da
22/03/20xx	22/03/20xx	1	Nuovo documento	Bianchi	A. Pesenato OdV	CDA

18.3. PROTOCOLLI PER DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (II)

18.3.1 Reati presupposto

La Legge 48/08[7] "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23.11.2001, e norme di adeguamento dell'ordinamento interno*", ha introdotto nel D.Lgs. n. 231/01 l'**art. 24 bis**, relativo ai reati informatici.

18.3.2 Caratteristiche generali dei reati di pirateria informatica

di seguito le fattispecie di reato che potrebbero in astratto essere consumati nell'ambito delle attività della società.

– Falsità in documento informatico o avente efficacia probatoria (art. 491-bis c.p.).

[7] Pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79.

- Punisce chi commette una delle falsità previste dal Titolo VII, Capo III c.p. e questa riguarda un documento informatico pubblico o privato, avente efficacia probatoria.[8]
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.). Si realizza nel caso in cui un soggetto, abusivamente, ossia eludendo una qualsiasi forma, anche minima di barrire ostative all'accesso, si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.[9]
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.). Si realizza nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.). Si realizza nel caso in un cui un soggetto nel caso in cui un soggetto, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici.
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quarter c.p.). Si realizza nel momento in cui un soggetto, fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Allo stesso modo compie un reato chiunque rivela, mediante qualsiasi mezzo di

[8] Si riportano le tipologie di reato associate: art. 476 c.p. Falsità materiale commessa dal pubblico ufficiale in atti pubblici; art. 477 c.p. Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative; art. 478 c.p. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati dal contenuto di atti; art. 479 c.p. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici; art. 480 c.p. Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative; art. 481 c.p. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità; art. 482 c.p. Falsità materiale commessa dal privato; art. 483 c.p. Falsità ideologica commessa dal privato in atto pubblico; art. 484 c.p. Falsità in registri e notificazioni; art. 485 c.p. Falsità in scrittura privata; art. 486 c.p. Falsità in foglio firmato in bianco. Atto privato; art. 487 c.p. Falsità in foglio firmato in bianco. Atto pubblico; art. 488 c.p. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali; art. 489 c.p. Uso di atto falso; art. 490 c.p. Soppressione, distruzione e occultamento di atti veri; art. 492 c.p. Copie autentiche che tengono luogo degli originali mancanti; art. 493 c.p. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

[9] A mero titolo di esempio, il reato potrebbe essere commesso nell'interesse o a vantaggio della società nel caso in cui determinati soggetti accedano abusivamente nel sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione alla gara d'appalto o accedano abusivo nel sistema informatico di un concorrente al fine di conoscere il portafoglio clienti.

informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al paragrafo precedente.
- Installazione di apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.). Si realizza nel caso in cui un soggetto, 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.
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.). Si realizza distruggendo, deteriorando o rendendo, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.
- 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.). Si realizza nel caso in cui un soggetto 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.
- Danneggiamento di sistemi informatici o telematici (art. 635-quarter c.p.). Si realizza nel caso in cui un soggetto, mediante le condotte di cui all'art. 635-bis, 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.
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.). Si realizza se il fatto di cui all'art. 635-quater 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.
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.). Si realizza nel caso in cui un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

18.3.3 Individuazione delle aree di attività a rischio

Con riferimento alla possibile commissione di reati informatici e di illeciti contro la proprietà intellettuale, sebbene la società non operi direttamente nel settore economico e professionale dell'informatica e della telematica, sussiste un rischio di accadimento delle fattispecie illecite indicate, con riferimento alle attività di gestione ed utilizzo delle reti e degli apparati informatici impiegati per lo svolgimento di qualsiasi attività riconducibile all'azienda. Ciò premesso, particolarmente a rischio sono le attività che prevedono:
- la gestione degli accessi logici ai sistemi informatici della Società, protetti o meno da sistemi di sicurezza, anche tramite internet;
- utilizzo di fotografie o materiale multimediale (es: musica e filmati) nel materiale di comunicazione della società;

– gestione di dotazioni e utilità aziendali (es. pc, autovetture ecc.);
– gestione della documentazione in formato digitale attraverso l'utilizzo di smart card /dispositivi di archiviazione digitale;
– gestione e regolamentazione degli accessi alla sala CED.

18.3.4 Destinatari

La presente parte speciale disciplina protocolli destinati a tutti coloro che sono dotati di una postazione informatica per lo svolgimento delle proprie mansioni o, in ogni caso, svolgono attività implicanti l'utilizzo di strumenti informatici. Particolarmente delicati risultano essere il ruolo dei soggetti, interni e/o esterni, cui è affidata la gestione del sistema informatico e di coloro che rivestono la qualifica di Amministratore di Sistema.
Sono altresì destinatari tutti i soggetti che utilizzano opere dell'ingegno (ad es. fotografie e filmati) nel materiale destinato alla comunicazione.
Sono a rischio le operazioni delle funzioni deputate alla trasmissione di documenti informatici alla Pubblica Amministrazione, ad esempio nell'ambito delle pratiche previdenziali o assicurative.
Tutti i soggetti individuati al presente paragrafo dovranno adeguarsi alle prassi operative e alle regole di condotta predisposte al fine di prevenire i reati di cui si tratta.

18.3.5 Regole di carattere generale

Tutti i Destinatari del Modello nello svolgimento o nell'esecuzione delle operazioni nell'ambito delle attività sensibili indicate nel paragrafo precedente, adottano regole di comportamento conformi ai principi generali di comportamento di seguito esposti al fine di prevenire il verificarsi dei reati informatici rilevanti per la Società e previsti dal Decreto.
Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella Parte Generale del presente Modello.
In particolare, è fatto divieto di:
– introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza;
– accedere ad un sistema informatico o telematico non possedendo le credenziali d'accesso o utilizzando le credenziali di altri colleghi abilitati;
– detenere, procurarsi o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
– utilizzare dispositivi tecnici o software non autorizzati e/o atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico;
– distruggere, danneggiare, cancellare, alterare informazioni, dati o programmi informatici altrui;
– riprodurre, diffondere, comunicare, o comunque mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un

sistema, o i dati e i programmi ad esso pertinenti, ovvero favorirne l'interruzione o l'alterazione del funzionamento.

Gli organi sociali ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate. In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- vigilare sui processi di approvvigionamento dei beni protetti da proprietà intellettuale;
- porre in essere correttamente e legalmente, in modo trasparente, tutte le attività di gestione delle risorse informatiche;
- monitorare e tener traccia dell'utilizzo del sistema informatico, dei programmi delle licenze e delle password personali e di sistema; rispettare la proprietà intellettuale di terzi nello svolgimento di attività, ivi comprese quelle di comunicazione o marketing, che possano comportare l'utilizzo di opere soggette al diritto d'autore.
- utilizzare correttamente le risorse informatiche aziendali a loro assegnate, evitando di lasciare incustodito e/o accessibile ad altri il proprio pc, ed informando tempestivamente il responsabile dell'Ufficio di appartenenza in caso di smarrimento o furto delle attrezzature informatiche aziendali;
- utilizzare le attrezzature informatiche aziendali unicamente per motivi d'ufficio.

18.3.6 Documenti diffusi fra gli organi sociali dell'azienda

In linea con i principi generali sopra riportati, la Società si è dotata ed ha debitamente formalizzato e divulgato al proprio interno i seguenti documenti:

- Organigramma generale e funzionale suddiviso per (*specificare*).
- Comunicazioni Interne di variazione dell'assetto organizzativo e di attribuzione di nuovi compiti e responsabilità.
- Codice Etico.
- Mission e Vision di gruppo.
- Sistema disciplinare di cui al CCNL ed al Modello.

18.3.7 Protocolli specifici

Oltre ai protocolli esistenti in Azienda e già citati in precedenza con riferimento ad altre fattispecie di rischio, che qui si intendono per richiamati, l'Azienda ha già predisposto ed adottato i seguenti strumenti:

- Codice Etico;
- Politiche di sicurezza e Privacy – Dipartimento IT, diffuso tra le funzioni aziendali e consegnato a tutti i neoassunti al momento della sottoscrizione del contratto;
- procedura per la gestione dei rapporti con la P.A., con riferimento alla trasmissione di documenti informatici aventi efficacia probatoria;
- Audit periodici sul sistema informatico;
- Misure tecniche e tecnologiche quali:
- URL Filtering;

– Gestione dei Proxy;
– Spam Monitoring;
– Installazione e aggiornamento di sistemi antivirus e firewall.

La società sta inoltre sviluppando la seguente misura:
– Previsione di protocolli organizzativi specifici destinati a regolamentare l'acquisto di software e l'approvvigionamento di altri beni protetti da proprietà intellettuale.
– Monitoraggio su software, programmi e applicazioni informatiche: devono essere definite le regole per l'utilizzo degli strumenti informatici aziendali e le attività di controllo su software, programmi, applicazioni informatiche installate su tali dispositivi, al fine di verificare che non vengano scaricate applicazioni potenzialmente utili alla commissione di attività illecite e / o contrarie alle disposizioni aziendali definite (es. manomettere il sistema informatico di terzi, accedere impropriamente al sistema dei pagamenti interno per finanziare la commissione di reati 231).
– Controllo sicurezza su accesso a sistemi: devono essere definiti criteri e regole di autorizzazione per l'accesso ai sistemi informatici aziendali; tali accessi devono essere costantemente monitorati in termini di utenti che vi accedono e attività consentite. Devono essere inoltre implementate adeguate misure di sicurezza che impediscano l'accesso al sistema informativo del Gruppo da parte di terzi non autorizzati (dotazione di firewall).
– Monitoraggio periodico sugli amministratori di sistema: devono essere poste in essere specifiche attività di controllo sull'attività degli amministratori di sistema e su software, programmi e applicazioni presenti sui loro dispositivi informatici.

La società sta inoltre sviluppando la seguente misura:
– previsione di protocolli organizzativi specifici destinati a regolamentare l'acquisto di software e l'approvvigionamento di altri beni protetti da proprietà intellettuale.

18.3.8 Flussi informativi e attività dell'Organismo di Vigilanza (OdV)

Per ciascun processo sensibile, il Responsabile Interno deve:
– tenere a disposizione dell'OdV ogni eventuale documentazione di supporto;
– segnalare all'OdV e richiedere la sua assistenza per ogni situazione che si ritenga non conforme alle regole aziendali in materia o laddove si evidenzi comunque una situazione di anomalia.

L'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello, fermo restando il dovere di osservare il divieto di comunicare e/o diffondere le informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste da forze di polizia, dall'autorità giudiziaria, da organismi di sicurezza o

da altri soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione di reato.

18.3.9 Linee guida di Confindustria del marzo 2014 [10]

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

Modalità di realizzazione del reato	Controlli preventivi
Art. 491 *bis* c.p. Falsificazione di documenti informatici da parte di enti che procedono a rendicontazione elettronica di attività. Cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi, allo scopo di eliminare le prove di un altro reato (es. l'ente ha ricevuto un avviso di garanzia per un reato e procede ad eliminare le tracce elettroniche del reato stesso). Falsificazione di documenti informatici contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti tra privati e PA (es. riduzione degli importi) o alterazione dei documenti in transito nell'ambito del SIPA (Sistema Informatizzato pagamenti della PA) al fine di aumentare gli importi dovuti dalla PA all'ente. Falsificazione di documenti informatici compiuta nell'ambito dei servizi di *Certification Authority* da parte di un soggetto che rilasci certificati informatici, aventi valenza probatoria, corrispondenti a false identità o attestanti falsi titoli professionali. Falsificazione di documenti informatici correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che queste risultino eseguite dai soggetti legittimi titolari dei dati (es. attivazione di servizi non richiesti).	Misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate (A.10.9.3); Misure di protezione dei documenti elettronici (es. firma digitale) (A.12.3.1); Procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali

[10] Scheda tratta da Linee Guida Confindustria 2014.

Modalità di realizzazione del reato	Controlli preventivi
Art. 615-*ter* c.p. Violazione dei sistemi informatici dei concorrenti per acquisire a scopo di spionaggio industriale la documentazione relativa ai loro prodotti/progetti. Tale condotta assume particolare rilievo per gli enti la cui attività è basata su brevetti/disegni/attività di R&S (es. *automotive*, *design*, moda, tecnologie, ecc.). Accesso abusivo a sistemi informatici di concorrenti allo scopo di acquisire informazioni concernenti la clientela utili per esempio per l'elaborazione di strategie di *marketing* (es. dati di consumo, aree geografiche di riferimento, banche dati, etc.). Accesso abusivo a sistemi di enti pubblici per l'acquisizione di informazioni riservate (es. amministrazione giudiziaria o finanziaria). Accesso abusivo a sistemi interbancari al fine di modificare le informazioni sul proprio conto registrate su tali sistemi. Accesso abusivo a sistemi aziendali protetti da misure di sicurezza, per attivare servizi non richiesti dalla clientela. Accesso abusivo ai sistemi che realizzano la fatturazione dei servizi ai clienti per alterare le informazioni e i programmi al fine di realizzare un profitto illecito. Accesso abusivo ai sistemi che elaborano le buste paghe per alterare i dati relativi alle voci di cedolino al fine di ridurre illecitamente le erogazioni nei confronti degli stessi e realizzare così un interesse o un vantaggio per l'ente. Accesso abusivo ai sistemi che gestiscono il credito di clienti di servizi pre-pagati per modificare i dati di credito e realizzare un profitto per l'ente (come ad esempio avviene nei settori delle telecomunicazioni).	L'accesso abusivo, oltre ad essere di per sé un illecito, può essere strumentale alla realizzazione di altre fattispecie criminose. I controlli predisposti per prevenire tale fattispecie di reato potrebbero pertanto risultare efficaci anche per la prevenzione di altri reati. Tra tali controlli si segnalano: 1. - adozione di procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche; - procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (A.8.3.3 e A.11.2.1); - aggiornamento regolare dei sistemi informativi in uso; - modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto (A.11.2.2, A.11.5.1 e A.11.5.2); - procedura per il controllo degli accessi (A.11.1.1); - tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali (A.10.10.1, A.10.10.3 , A.10.10.4, A.10.10.2); - definizione e attuazione di un processo di autorizzazione della direzione per le strutture di elaborazione delle informazioni (A.6.1.4).

Modalità di realizzazione del reato	Controlli preventivi
Art. 615-*quater* c.p. Detenzione e utilizzo di *password* di accesso a siti di enti concorrenti al fine di acquisire informazioni riservate. Detenzione ed utilizzo di *password* di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse dell'azienda, anche in violazione di leggi sulla *privacy* o dello statuto dei lavoratori. Detenzione abusiva di codici di accesso a sistemi informatici dell'amministrazione giudiziaria o finanziaria al fine di acquisire informazioni riservate su procedimenti penali/amministrativi che coinvolgano l'azienda. 2. Diffusione abusiva di numeri seriali di telefoni cellulari altrui al fine della clonazione degli apparecchi.	Inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni (A.6.1.5). Procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro (A.8.3.3 e A.11.2.1).
Art. 617-*quater* e 617-*quinquies* c.p. Intercettazione fraudolenta di comunicazioni di enti concorrenti nella partecipazione a gare di appalto o di fornitura svolte su base elettronica (*e-marketplace*) per conoscere l'entità dell'offerta del concorrente. Tale tipologia di gestione degli acquisti/gare è frequente nell'ambito della PA. Impedimento o interruzione di una comunicazione al fine di evitare che un concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara. Intercettazione fraudolenta di una comunicazione tra più parti al fine di veicolare informazioni false o comunque alterate, ad esempio per danneggiare l'immagine di un concorrente Intercettazione delle comunicazioni telematiche della clientela al fine di analizzarne le abitudini di consumo Impedimento del regolare funzionamento di apparecchi deputati al controllo delle emissioni prodotte da impianti, ad esempio al fine di occultare il superamento dei limiti consentiti e, conseguentemente, la revoca di autorizzazioni amministrative	Definizione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3). Elaborazione di procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione (A.7.2.2); Utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse (A.9.1.1). Allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione (A.9.2.5 e A.10.8.3). Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato (A.10.1.1 e A.10.1.2). Previsione di controlli su: - rete aziendale e informazioni che vi transitano (A.10.6.1); - instradamento (*routing*) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza (A.11.4.7);

Modalità di realizzazione del reato	Controlli preventivi
Installazione di apparecchiature atte ad intercettare ed impedire comunicazioni informatiche commessi dal personale incaricato della gestione degli apparati e dei sistemi componenti l'infrastruttura di rete aziendale.	- installazione di *software* sui sistemi operativi (A.12.4.1). Predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).
Art. 615-*quinquies*, 635 *bis*, 635 *quater* c.p. Danneggiamento di informazioni, dati e programmi aziendali di un concorrente causato mediante la diffusione di virus o altri programmi malevoli commessa da soggetti che utilizzano abusivamente la rete o i sistemi di posta elettronica aziendali. Danneggiamento di informazioni, dati, programmi informatici aziendali o di sistemi informatici di terzi, anche concorrenti, commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza. Danneggiamento dei sistemi su cui i concorrenti conservano la documentazione relativa ai propri prodotti/progetti allo scopo di distruggere le informazioni e ottenere un vantaggio competitivo. Danneggiamento delle infrastrutture tecnologiche dei concorrenti al fine di impedirne l'attività o danneggiarne l'immagine. Con riferimento a tali condotte, sono da considerarsi maggiormente esposti al rischio gli enti la cui attività dipende strettamente dalle infrastrutture tecnologiche, come ad esempio avviene nell'e-*commerce* o e-*banking*	Formalizzazione di regole al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3). Procedure per l'etichettatura e il trattamento delle informazioni in base allo schema di classificazione adottato dall'ente (A.7.2.2). Controlli di individuazione, prevenzione e ripristino al fine di proteggere da *software* dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema (A.10.4.1). Presenza di misure per un'adeguata protezione delle apparecchiature incustodite (A.11.3.2). Previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business (A.11.6.2). Procedure di controllo della installazione di *software* sui sistemi operativi (A.12.4.1). Procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).
Art. 635-*ter*, 635 *quinquies* c.p. Danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), da parte di dipendenti di enti coinvolti a qualunque titolo in procedimenti o indagini giudiziarie.	Formalizzazione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (A.7.1.3). Procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione (A.7.2.2).

Modalità di realizzazione del reato	Controlli preventivi
Danneggiamento di informazioni, dati e programmi informatici utilizzati da enti pubblici commesso dal personale incaricato della gestione dei sistemi di clienti della PA	Controlli di individuazione, prevenzione e ripristino al fine di proteggere da *software* dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema (A.10.4.1). Procedure di controllo della installazione di *software* sui sistemi operativi (A.12.4.1). Procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi (A.12.6.1).
Art. 640-*quinquies* c.p. Rilascio di certificati digitali da parte di un ente certificatore senza che siano soddisfatti gli obblighi previsti dalla legge per il rilascio di certificati qualificati (es. identificabilità univoca del titolare, titolarità certificata), con lo scopo di mantenere un alto numero di certificati attivi. Aggiramento dei vincoli imposti dal sistema per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre così un guadagno all'ente.	Predisposizione di misure volte alla protezione dei documenti elettronici (es. firma digitale). Elaborazione di procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali.

18.4. PROTOCOLLI PER DELITTI DI CRIMINALITÀ ORGANIZZATA (IV)

18.4.1 Reati presupposto

La Legge n. 94/09 "Disposizioni in materia di sicurezza pubblica", approvata lo scorso 15.07.09 ha introdotto nel D.Lgs. 231/01 la previsione di cui all'art. 24 ter "Delitti di Criminalità Organizzata". In particolare è prevista la responsabilità amministrativa degli enti nel caso di commissione dei seguenti reati: associazione a delinquere (art. 416 c.p.), associazione per delinquere di tipo mafioso anche straniera (art. 416 bis c.p.), scambio elettorale politico mafioso (art. 416 ter c.p.), sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.), associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74, D.P.R. 309/90), produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope (art. 73, D.P.R. 309/90), illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della Legge 18 aprile 1975, n. 110 (art. 407, comma 2, lettera a), n. 5 c.p.p.).