PARTE SPECIALE

Allegato II

REATI DI CRIMINALITA' ORGANIZZATA

(Art. 24 ter del D.lgs 231/2001)

Si provvede di seguito a fornire una breve descrizione dei reati indicati negli art. 24 ter del d.lgs 231/2001 ed appartenenti alla macro categoria dei reati di criminalità organizzata.

Associazione per delinquere (art. 416 bis c.p.)

Tale ipotesi di reato si configura nel caso in cui tre o più persone si associano allo scopo di commettere più delitti. Coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, solo per tale fatto, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.

Associazione di tipo mafioso (art. 416 bis c.p.)

Il più grave reato associativo previsto dall'art. 416 bis c.p. differisce dal precedente soltanto per la tipologia dell'associazione criminale.

Scambio elettorale politico mafioso (art. 416 ter c.p.)

La pena stabilita dal primo comma dell'art. 416 bis c.p. si applica anche a chi ottiene la promessa di voti in cambio di erogazione di denaro.

Sequestro di persona a scopo di rapina od estorsione (art. 630 c.p.)

Tale ipotesi di reato si configura a carico di chiunque sequestri una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione ed è punita con la reclusione da venticinque a trenta anni. Se dal sequestro deriva comunque la morte, quale conseguenza non voluta del reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta. Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.

Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990)

Detto che i requisiti della partecipazione a questo tipo di associazione criminale sono i medesimi di cui all'art. 416 c.p. è da tener presente che l'art. 74 D.P.R. n. 309/1990, richiamando l'art. 73 D.P.R. include tra i reati-fine il fatto di chi " senza l'autorizzazione di cui all'art. 17 coltiva, produce, fabbrica, estrae, raffina, vende, offre, mette in vendita, cede o riceve, a qualsiasi titolo, distribuisce, commercia , acquista, trasporta, esporta, importa, procura ad altri, invia, passa o spedisce in transito, consegna per qualunque scopo o comunque illecitamente detiene, fuori dalle ipotesi previste dall'art. 75, sostanze stupefacenti o psicotrope".

AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree che potrebbero possedere un potenziale rischio sono:

- Convenzioni con il Comune di Velletri e con la ASL per la gestione dei parcheggi;
- Trasporto valori;
- appropriazione indebita di somme di denaro non riversate o rimborso di somme non dovute, esplicabili nelle attività quali svuotamento parcometri, trasporto valori, versamento su ccpp;
- Riconciliazioni bancarie e contabilità del ciclo attivo e passivo;
- Rilascio permessi disabili, permessi residenti, permessi zona a traffico limitata, altri permessi;
- Ordine on line quotidiani di farmaci da grossisti, programmazione fabbisogno e smistamento farmaci, nonché di acquisti di materie prime per preparazioni galeniche;

DESTINATARI: PRINCIPI GENERALI DI COMPORTAMENTO

Il presente allegato 2 si riferisce a comportamenti posti in essere da esponenti aziendali, partner, fornitori e consulenti.

Obiettivo del presente Allegato 2 è che tutti i Destinatari si attengano, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati precedentemente descritti, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei reati di cui alla presente Parte Speciale.

Nell'espletamento delle attività aziendali, in particolare, è espressamente vietato ai Destinatari di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato di cui alla presente Parte Speciale.

In particolare è necessario:

- mantenersi costantemente aggiornati ed informati sulle regole ed i presidi vigenti all'interno della struttura Velletri Servizi e posti a prevenzione dei reati di cui alla presente Parte Speciale;
- approfondire la conoscenza della Clientela al fine di valutare la coerenza e la compatibilità dell'operazione impartita con il profilo del Cliente;
- evidenziare ed immediatamente segnalare le operazioni poste in essere da un soggetto in nome o a favore di terzi in assenza di legami familiari o relazioni commerciali idonee a giustificarle ovvero anche le operazioni poste in essere da soggetti terzi in favore di Clienti in assenza di valide ragioni giustificatrici;

- mantenere aggiornati tutti i dati relativi ai rapporti con il Cliente al fine di consentire una valida valutazione del suo profilo economico/finanziario;
- mantenere traccia di tutte le varie fasi dei processi aziendali.
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di Collaboratori esterni, Clienti, Partner;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette e, potenzialmente, parte di movimenti finanziari per gli scopi delittuosi di cui alla presente Parte Speciale;

Ai Destinatari è inoltre fatto divieto di:

- promuovere, costituire od organizzare associazioni con altri soggetti allo scopo di commettere delitti;
- in ogni caso, incoraggiare, sostenere o partecipare ad associazioni per delinquere, in particolare se di stampo mafioso;

PARTE SPECIALE

Allegato III

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

(Art. 24 bis del D.lgs 231/2001)

Si provvede di seguito a fornire una breve descrizione dei reati indicati negli art. 24 bis del d.lgs 231/2001 ed appartenenti alla macro categoria dei reati informatici e trattamento illecito di dati.

Accesso abusivo ad un sistema informatico e telematico (art. 615 ter c.p.)

Tale ipotesi di reato si configura nel caso in cui un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Il soggetto che promuove tale reato è punito con la reclusione fino a tre anni.

La pena è rappresentata dalla reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora tali fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi un'effettiva lesione alla stessa.

L'art. 1 della Convenzione di Budapest chiarisce che per "sistema informatico" si considera "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico", che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".

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

Tale ipotesi di reato si configura quando un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo. Tale condotta è punita con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)

Tale ipotesi di reato si configura quando 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, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

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

Tale ipotesi di reato si configura a carico di chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Per tale condotta è prevista la reclusione da sei mesi a quattro anni.

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

Installazione di apparecchiature o soppressione di contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.)

Tale ipotesi di reato si configura a carico di chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Per tale condotta è prevista la reclusione da uno a quattro anni.

Danneggiamento di sistemi informatici o telematici (art. 635 bis c.p.)

Salvo che il fatto costituisca più grave reato, tale ipotesi si configura quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici. Tale condotta è punita, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

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

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

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, la pena è rappresentata dalla reclusione da tre a otto anni.

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

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

Salvo che il fatto non costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni programmi, rende, il tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

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

Danneggiamento di sistemi informatici o telematici (art. 635 quinques c.p.)

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

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

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, 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, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree che potrebbero possedere un potenziale rischio sono:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno (internet);
- gestione e protezione delle reti;
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);
- installazione di programmi e dispositivi;
- gestione del processo di conservazione sostitutiva documentale.

DESTINATARI: PRINCIPI GENERALI DI COMPORTAMENTO

Il presente allegato si riferisce a comportamenti posti in essere da esponenti aziendali, partner, fornitori e consulenti.

Obiettivo del presente Allegato è che tutti i Destinatari si attengano, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno

dei reati precedentemente descritti, a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei reati di cui alla presente Parte Speciale.

Nell'espletamento delle attività aziendali, in particolare, è espressamente vietato ai Destinatari di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato di cui alla presente Parte Speciale.

In particolare è fatto divieto di:

- alterare documenti informatici, pubblici o privati, 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;
- 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;
- istallare 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.

I Destinatari, quindi, devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;

- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione della Velletri Servizi;
- in caso di smarrimento o furto, informare tempestivamente gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
- evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dalla Velletri Servizi o la cui provenienza sia dubbia;
- evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione della società stessa;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
- evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione della società;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.