Parte Speciale "M"

Delitti in materia di strumenti di pagamento diversi dai contanti

INDICE

1. – Premessa

2. – I reati di cui all'art. 25-*octies.*1 del Decreto

2.1. – Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter* c.p.)

2.2. – Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.)

2.3. - Trattamento sanzionatorio per le fattispecie di cui all'art. 25-*octies.*1 del Decreto

3. - Le aree a rischio reato ed i presidi di controllo esistenti

4. - I Compiti dell'Organismo di Vigilanza

1. – PREMESSA

L'articolo 25-*octies*.1 è stato introdotto nel sistema della responsabilità da reato degli Enti dall'articolo 3 del D. Lgs. 8 novembre 2021, n. 184.

In particolare, il predetto decreto – composto da sei articoli – ha recepito la Direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, al fine di adeguare la normativa nazionale a quella euro-comunitaria del Parlamento e del Consiglio Europeo.

La finalità della presente parte speciale è quella di intensificare gli strumenti di lotta alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti e ciò per due ordini di ragioni specifiche:

i) bloccare la crescita della criminalità organizzata e di conseguenza la diversificazione del novero delle attività criminose;

ii) implementare lo sviluppo del mercato unico digitale e di conseguenza accrescere la fiducia che i consumatori ripongono nell'economia globale.

Inoltre, il legislatore ha ritenuto necessario introdurre i riportati nuovi reati-presupposto in quanto le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti hanno assunto, nel corso degli ultimi anni, un ragguardevole sviluppo transfrontaliero, portando come conseguenza immediata l'esigenza di garantire una normativa comune a tutti gli Stati membri, al fine di agevolare la cooperazione tra le diverse Autorità competenti.

Difatti, il legislatore nazionale, al fine di armonizzare la disciplina italiana a quella comunitaria, ha predisposto misure sanzionatorie (anche penalistiche) efficaci e repressive dei fenomeni summenzionati, attraverso la modifica di fattispecie di reato quali quelle di cui agli artt. 493 *ter* e 640 *ter* c.p. e l'inserimento *ex novo* della fattispecie di cui all'art. 493 *quater* c.p.

Di nuovo conio, all'art. 1 del D. lgs. n. 184/2021, si rinvengono altresì definizioni euro-comunitarie come "*strumenti di pagamento diverso dai contanti, dispositivo, oggetto o record protetto, mezzo di scambio digitale e valuta virtuale",* che il legislatore utilizza appositamente per allargare la maglia della rilevanza penale delle fattispecie sinora richiamate.

Infine, è importante sottolineare come questo nuovo intervento legislativo abbia inciso principalmente sull'oggetto della tutela cui mirano le norme esaminate, al fine di estenderlo a tutti quegli strumenti di

pagamento diversi dai contanti e, di conseguenza, accrescere inevitabilmente il sistema di *compliance* aziendale.

2. – I REATI DI CUI ALL'ART. 25-*OCTIES.*1 DEL DECRETO

2.1. - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter* c.p.)

Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità' di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.

La norma in esame è volta alla tutela del patrimonio, oltre che alla corretta circolazione del credito.

È doveroso segnalare come il legislatore abbia voluto punire alla stessa guisa chi si avvalga di carte di credito di cui non è titolare al fine di trarne profitto (e dunque senza averla rubata, ma anche

solamente avendola trovata) e chi falsifica tali strumenti sempre al fine di trarne profitto. Nell'ultima ipotesi prospettata viene punita anche la cessione delle carte falsificate ed ogni altra condotta atta a metterle comunque in circolazione.

Il reato si consuma nel momento esatto in cui vengono utilizzate le carte ovvero, rispettivamente, nel momento in cui l'agente le falsifichi o le ceda a terzi. Dunque, al fine di integrare la fattispecie di reato non è richiesto l'effettivo conseguimento di un profitto, bastando bensì che venga accertato il dolo specifico.

Nonostante tale anticipazione della tutela penale, il legislatore ha in tal modo voluto rendere configurabile e punibile anche il mero tentativo.

Ebbene, la norma in esame è stata di recente modificata in attuazione della Direttiva (UE) 2019/713 – relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti – volta a sanzionare anche chi utilizzi "ogni altro strumento di pagamento diverso dai contanti" per la realizzazione della condotta sopra enunciata.

Di conseguenza, il legislatore - pur mantenendo inalterato il regime sanzionatorio - ha voluto estendere a tutti gli strumenti di pagamento "diversi" dai contanti l'ascrivibilità della fattispecie di reato.

Infine, ai sensi dell'articolo 1 del decreto legislativo n. 184/2021, si identificano come strumenti di pagamento diversi dai contanti: ogni dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta avente corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali.

Per le altre definizioni, meno rilevanti ai fini della presente trattazione, si rimanda integralmente alla norma citata.

2.2. – Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

La norma in esame è stata introdotta ex novo dal D. Lgs. n. 184/2021 al fine di approntare ulteriori strumenti di repressione efficaci o comunque idonei a garantire la salvaguardia e la sicurezza degli scambi economici e, indirettamente, a tutelare tutti i soggetti attivi nel mercato da qualsivoglia frode posta in essere.

Si tratta di un reato comune, punito a titolo di dolo specifico, in quanto le condotte descritte assumono rilevanza penale qualora compiute al precipuo fine di utilizzare o consentire ad altri di utilizzare uno dei dispositivi indicati dalla norma.

Inoltre, il secondo comma dell'articolo è stato costruito dal legislatore sulla falsariga di quanto disciplinato dall'art. 493 ter c.p., ossia prevendo la confisca – in caso di condanna o di patteggiamento – delle apparecchiature, dei dispositivi e/o dei programmi informatici elencati dalla norma.

È doveroso sottolineare come l'inserimento della nuova ipotesi di reato nel novero di quelli presupposto ai sensi del D.Lgs. n. 231/2001 sia frutto di una precisa scelta di politica criminale, dando attuazione all'art 7 della citata Direttiva comunitaria, il quale prevede l'adozione da parte degli Stati membri di misure idonee a sanzionare le persone giuridiche nel cui vantaggio o interesse siano stati commessi i reati di cui all'art. 3, par. 1 e 5 e di cui all'art 4.

2.5. - Trattamento sanzionatorio per le fattispecie di cui all'art. 25-*octies.*1 del Decreto

In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di cui all'articolo 493-*ter* la sanzione pecuniaria da 300 a 800 quote;

b) per il delitto di cui all'articolo 493-*quater* e per il delitto di cui all'articolo 640 *ter* nell'ipotesi aggravata della realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a 500 quote.

Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la pubblica fede, contro il patrimonio o comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore a dieci anni, la sanzione pecuniaria sino a 500 quote;

b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote;

Nei casi di condanna per uno dei delitti di cui ai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

3. – <u>LE AREE A RISCHIO REATO ED I PRESIDI DI CONTROLLO ESISTENTI</u>

La presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi cui i destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

In tutte le aree "a rischio reato" qui considerate occorre osservare i seguenti Presidi di Controllo Generali (a cui si aggiungono Presidi di Controllo Specifici in relazione a singole attività sensibili o categorie di attività sensibili):

1) rispetto del Codice Etico;

2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, con particolare riguardo ai temi relativi alla prevenzione dei fenomeni di frodi e falsificazione di mezzi di pagamento diverso dai contanti, nei confronti delle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;

3) diffusione del Modello tra le risorse aziendali, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet della Società;

4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito intranet della Società o messa a disposizione in formato cartaceo o telematico;

5) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari (ad es., fornitori, consulenti, appaltatori), si impegnano a rispettare le previsioni del Decreto;

6) previsione e attuazione del Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi;

7) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della Società, di impegno al rispetto dello stesso, incluso il Codice Etico;

8) implementazione di un sistema di dichiarazioni periodiche (almeno semestrali) da parte dei Responsabili Interni con le quali si fornisce evidenza del rispetto e/o della inosservanza del Modello (o, ancora di circostanze che possono influire sull'adeguatezza ed effettività del Modello);

9) creazione di una "Sezione 231" all'interno della intranet aziendale, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello della Società (ad es., Modello, Codice Etico, Protocolli aziendali in esso richiamati);

10) individuazione ed attuazione di specifici programmi di controllo interno anche con riguardo alla materia in esame, con particolare attenzione alla gestione dei pagamenti diversi dai contanti, agli accordi/joint venture con altre imprese, ai rapporti *intercompany*, tenendo in particolare conto della congruità economica di eventuali investimenti;

11) evidenza delle attività e dei controlli svolti;

12) informazione diretta ai destinatari in ordine al dovere di segnalare all'OdV eventuali operazioni sospette o eventuali infrazioni delle regole comportamentali sopra precisate di cui siano venuti a conoscenza in occasione dell'attività professionale svolta;

13) regole di *corporate governance* adottate dalla Società;

14) osservanza delle procedure aziendali che prevedono l'analisi di tutti i soggetti che hanno rapporti con la Società avuto particolare riguardo alle procedure di selezione dei fornitori;

15) osservanza di ogni altra normativa interna relativa alla selezione e verifica delle controparti contrattuali;

16) osservanza di ogni altra documentazione relativa al sistema di controllo interno in essere nella Società.

17) rispetto di regole, procedure e istruzioni operative adottate dalla Società in tema di sicurezza di dispositivi informatici.

Area a rischio n.1: rapporti con fornitori, consulenti e terzi

Attività sensibili:

1) relazioni con fornitori, consulenti, partners, sia a livello nazionale che internazionale;

2) rapporti di natura contrattuale con soggetti diversi da quelli di cui al punto precedente con cui la Società intrattiene delle relazioni, sia in Italia che all'estero;

3) rapporti con le consociate;

4) gestione dell'anagrafica Fornitori/Consulenti;

5) selezione dei fornitori/consulenti.

Reati ipotizzabili:

-Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter* c.p.)

-Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.)

Ulteriori presidi (**specifici**) di controllo:

1) identificare l'attendibilità dei fornitori e, più in generale, dei partner commerciali e finanziari, al fine di verificarne l'affidabilità anche sotto il profilo della correttezza e tracciabilità delle transazioni economiche con gli stessi, evitando di instaurare o proseguire rapporti con soggetti che non presentino o mantengano nel tempo adeguati requisiti di trasparenza e correttezza;

2) monitorare nel tempo il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità e onorabilità;

3) selezionare i professionisti e partner sulla base di criteri di trasparenza, di economicità e correttezza, garantendo la tracciabilità delle attività atte a comprovare i menzionati criteri;

4) effettuare una attività di *due diligence* finalizzata all'accertamento delle professionalità, competenze ed esperienze del professionista, nonché atta a identificare eventuali condizioni di incompatibilità e conflitto di interessi, nonché, la data di costituzione e degli anni di esercizio della Società a cui il professionista fa capo;

5) accertare i requisiti di onorabilità del professionista e verifica della eventuale sussistenza di condanne penali o sanzioni a carico dello stesso;

6) accertare la località della sede o residenza del professionista, la quale non deve essere situata in paesi a regime fiscale privilegiato, salvo che si tratti di contratti da stipularsi con professionisti residenti in paesi a regime fiscale privilegiato e tale paese sia il medesimo in cui saranno svolte le prestazioni professionali;

7) determinare i requisiti minimi in possesso dei soggetti offerenti e fissare i criteri di valutazione delle offerte nei contratti standard;

8) identificare l'organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità;

9) garantire la predisposizione e l'aggiornamento dell'anagrafica dei fornitori;

10) creazione dell'anagrafica Fornitori/Consulenti, nella quale inserire i fornitori e i consulenti della Società, assicurandone la previa qualificazione mediante l'accertamento dei requisiti di professionalità ed onorabilità;

11) formalizzazione dei requisiti da richiedere ai fornitori/consulenti e dei criteri da utilizzare nella relativa selezione, nonché delle ragioni che giustificano eventuali deroghe dai requisiti e criteri suddetti;

12) individuazione delle risorse deputate: a) a selezionare i potenziali nuovi fornitori/consulenti b) a formalizzare l'accordo negoziale; c) a gestire l'anagrafica Fornitori/Consulenti; d) a gestire i pagamenti delle fatture emesse dai fornitori/consulenti;

13) richiesta, ove possibile, di almeno due preventivi in sede di selezione dei fornitori/consulenti;

14) archiviazione della documentazione inviata dai potenziali candidati e concernente il rispetto dei requisiti richiesti;

15) formalizzazione delle ragioni per le quali è stato scelto un determinato fornitore/consulente/appaltatore;

16) emissione dell'ordine di acquisto nei confronti dei soli fornitori già presenti nell'anagrafica Fornitori;

17) inserimento nei contratti di appalto/fornitura e negli accordi con i consulenti di una clausola volta ad assicurare il rispetto del Modello e del Codice Etico della Società. Più precisamente, informazione rivolta ai consulenti e ai partner circa l'adozione del Modello e del Codice Etico da parte della Società la cui conoscenza e il cui rispetto costituirà obbligo contrattuale a carico di tali soggetti. In particolare, nell'espletamento delle attività considerate a rischio, gli esponenti aziendali, in via diretta, e i consulenti e i partner, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la Società, dovranno attenersi ai seguenti principi generali di condotta:

(I) astenersi dal tenere comportamenti tali da integrare le fattispecie previste nella presente Parte Speciale;

(II) astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

(III) 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 fornitori/clienti/partner anche stranieri;

(IV) non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza a organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente delle frodi e delle falsificazioni di qualsivoglia strumento e/o mezzo di pagamento;

(V) non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;

(VI) effettuare un costante monitoraggio dei flussi finanziari aziendali.

Area a rischio n. 2: Processo di accertamento circa l'utilizzo di strumenti di pagamento diversi dai contanti

Attività sensibili:

a) verifica in ordine al novero dei soggetti legittimati all'utilizzo delle carte di credito/debito aziendali ed alle limitazioni agli stessi eventualmente imposte nell'ambito del suddetto utilizzo;
b) controllo, autorizzazione e/o approvazione postuma dei pagamenti effettuati tramite strumenti diversi dai contanti;
c) identificazione dei ruoli e delle responsabilità degli addetti all'esecuzione e alla verifica dei pagamenti sotto qualsivoglia forma;
d) gestione dei pagamenti online (come ad esempio attraverso valuta virtuale) effettuati in favore di soggetti interni o soggetti terzi;

Reati ipotizzabili:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter* c.p.)

Ulteriori presidi (**specifici**) di controllo:

i) istituire un registro delle carte di credito/debito aziendali, in cui vengano annotati i nominativi dei soggetti destinatari delle carte medesime ed eventuali limiti al relativo utilizzo;

ii) predisporre un registro in cui vengano annotate le figure aziendali abilitate alla effettuazione di pagamenti o all'utilizzo dei sistemi di pagamento digitali, con l'indicazione di eventuali limiti di spesa o di utilizzo;

iii) porre in essere attività di monitoraggio dei pagamenti effettuati per il tramite dei suddetti strumenti;

iv) registrare e/o conservare documentazione attestante le transazioni ed i pagamenti effettuati in nome e per conto della Società attraverso i suddetti strumenti;

v) verificare "a campione" la regolarità delle transazioni e dei pagamenti eseguiti per il tramite dei suddetti strumenti, anche mediante consultazione della documentazione giustificativa (soprattutto in caso di "spese vive") e/o autorizzativa in base al sistema di poteri e deleghe in essere.

Inoltre, è severamente **vietato:**

- prelevare illegittimamente denaro contante utilizzando carte di credito/debito aziendali;
- utilizzare, per l'effettuazione di pagamenti in nome e per conto della Società, uno strumento di pagamento diverso dai contanti di provenienza illecita o comunque di non comprovata legittimità;
- contraffare o distribuire strumenti di pagamenti aziendali;

- violare i sistemi di informazione o manipolare i dati sensibili dello strumento di pagamento aziendale diverso dai contanti, al fine di ottenere indebitamente un arricchimento per sé o per altri.

Area a rischio n. 3: Processo tecnico di verifica di tutte le attività aziendali svolte tramite l'utilizzo di apparecchiature, dispositivi e/o programmi informatici aziendali.

Attività sensibili:

a) gestione dei programmi informatici aziendali, al fine di assicurarne il funzionamento e la manutenzione;

b) monitoraggio dei programmi e/o dei dispositivi informatici utilizzati al fine di compiere pagamenti *online*;

c) gestione delle apparecchiature informatiche idonee alla diffusione di dati sensibili circa l'effettuazione di pagamenti con mezzi diversi dai contanti;

d) utilizzo di sistemi informatici di gestione e controllo degli adempimenti fiscali e amministrativi.

Reati ipotizzabili:

- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.)

Ulteriori presidi (**specifici**) di controllo:

1) divieto posto a carico di tutti i destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato tra quelle sopra considerate;

- violare i principi di comportamento previsti nella presente Parte Speciale, nonché le regole e prassi aziendali di interesse;

2) individuazione e adozione di misure adeguate di sicurezza di natura organizzativa, fisica e logistica, in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o distruzione delle risorse informatiche e che si pongano quale obiettivo quello di:

- tutelare la sicurezza delle informazioni;
- prevedere eventuali controlli di sicurezza specifici per tipologia di asset;
- prevedere eventuali controlli di sicurezza destinati a indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali.

3) obbligo per tutti i destinatari del presente Modello di rispettare i principi comportamentali posti a presidio del rischio di commissione dei delitti informatici, volti ad assicurare l'osservanza dei seguenti parametri di sicurezza del patrimonio informativo della Società previsti dai principali standard internazionali in tema di sicurezza delle informazioni:

- riservatezza intesa come garanzia che una informazione o un pagamento siano accessibile solo a chi è autorizzato;

- integrità intesa come salvaguardia dell'accuratezza e della completezza dell'informazione o del pagamento;

- disponibilità intesa come garanzia che gli utenti autorizzati abbiano accesso alle informazioni ed all'effettuazione del pagamento, quando richiesto.

In particolare, è vietato:

(*a*) contraffare le forme di pagamento materiali (carte di credito, assegni etc.) e immateriali (valute virtuali) al fine di eseguire un profitto personale o per conto di terzi;

(b) ottenere credenziali di accesso ai dispositivi informatici o telematici aziendali dei clienti o di terze parti con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;

(c) manomettere, sottrarre o distruggere i sistemi di informazione dei dati informatici al fine di effettuare il trasferimento illegale di denaro della società o dei clienti;

(d) sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei dispositivi/sistemi informatici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

I destinatari del Modello sono tenuti a rispettare scrupolosamente tutte le norme vigenti, e in particolare:

- utilizzare i dispositivi, programmi o apparecchiature informatiche assegnati esclusivamente per l'espletamento della propria attività;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- garantire la tracciabilità dei documenti prodotti al fine di effettuare qualsivoglia pagamento;

4) formazione e addestramento periodico in favore dei dipendenti, diversificato in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore dei destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali propedeutiche all'effettuazione di qualunque tipologia di pagamento;

4. – I COMPITI DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i c.d. reati di cui all'art. 25-*octies.*1 del D. Lgs. n. 231/2001 sono i seguenti:

- proporre che vengano emanate e aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale;

- monitorare costantemente l'efficacia delle procedure aziendali che la Società adotta.

- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti l'OdV può accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti, nonché acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

In particolare, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici della presente Parte Speciale ovvero alle procedure aziendali attinenti alle aree sensibili sopra individuate.