PARTE SPECIALE “P”

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSO DAI CONTANTI

INDICE

1. *Le fattispecie dei delitti in materia di strumenti di pagamento diversi dai contanti richiamate dal d.lgs. n. 231/2001*

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del d.lgs. n. 231/2001 è collegato il regime di responsabilità a carico della Società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal Decreto.

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. n. 231/2001, riportiamo, qui di seguito, una breve descrizione dei reati richiamati dall'art. 25-*octies.1* del d.lgs. n. 231/2001.

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

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.

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.)

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.

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.

2. Le "attività sensibili" ai fini del d.lgs. n. 231/2001

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. n. 231/2001.

L'analisi dei processi aziendali di Geolog, svolta nel corso del progetto ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-*octies.1* del d.lgs. n. 231/2001 compresi alcuni processi che potrebbero essere considerati "strumentali" alla commissione dei reati c.d. "presupposto". Qui di seguito sono elencate le attività sensibili esaminate:

Gestione dei rapporti con fornitori, consulenti e terzi

Si tratta delle attività relative alla selezione dei fornitori/consulenti, alla gestione degli approvvigionamenti, al controllo dei pagamenti in entrata ed in uscita erogati con riferimento a tutte le categorie di pagamento erogati dalla Società.

Gestione del processo di accertamento circa l'utilizzo di strumenti di pagamento diversi dai contanti

Si tratta di attività inerenti la verifica dei soggetti legittimati all'utilizzo dei mezzi di pagamento messi a disposizione dalla Società e, all'individuazione dei ruoli e/o responsabilità degli addetti all'esecuzione dei pagamenti sotto qualsivoglia forma.

Processo di verifica delle attività aziendali svolte tramite l'utilizzo di apparecchiature, dispositivi e/o programmi informatici aziendali

Si tratta di attività concernenti la gestione e il monitoraggio dei programmi e dei dispositivi informatici utilizzati al fine di effettuare i pagamenti aziendali.

3. *Presidi di controllo*

I presidi di controllo generali che la Società ha deciso di adottare al fine di prevenire il c.d. "rischio reato" nelle attività sensibili perseguite – ovvero quelle nel cui ambito è effettivamente sussistente il rischio di commissione delle fattispecie delittuose – sono molteplici ed elencati di seguito:

1) Codice Etico;
2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle 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) 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) ove necessario, documentazione scritta, tracciabilità ed archiviazione dei contatti con la PA;

10) 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).

La Società, inoltre, ha predisposto delle linee guida da seguire nell’adozioni dei comportamenti idonei a prevenire il rischio reato attraverso degli *standard* basilari:

- **Procedure**: gli *standard* si fondano sull’esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: gli *standard* si fondano sul principio secondo cui: i) ogni operazione relativa all’attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell’attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.
- **Segregazione dei compiti**: gli *standard* si fondano sulla separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Procure e deleghe**: gli *standard* si fondano sul principio secondo il quale i poteri autorizzativi e di firma assegnati debbano essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all’interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese.

3.1 Presidi di controllo specifici e connesse procedure con riferimento ad ogni singola attività sensibile.

Come evidenziato nel paragrafo precedente, all’esito della fase di “*risk assessment”* sono state individuate le c.d. attività sensibili alle quali discendono i presidi di controllo specifici in relazione a singole attività o categorie di attività sensibili:

Attività n. 1 Gestione dei rapporti con fornitori, consulenti e terzi

- 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;
- monitorare nel tempo il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità e onorabilità;
- 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;
- 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;
- accertare i requisiti di onorabilità del professionista e verificare l’eventuale sussistenza di condanne penali o sanzioni a carico dello stesso;
- 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;
- determinare i requisiti minimi in possesso dei soggetti offerenti e fissare i criteri di valutazione delle offerte nei contratti standard;
- identificare l'organo/unità responsabile dell'esecuzione del contratto, con indicazione di compiti, ruoli e responsabilità;
- 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;
- 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.

Attività n. 2 Gestione del processo di accertamento circa l'utilizzo di strumenti di pagamento diversi dai contanti

- 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;
- 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;
- porre in essere attività di monitoraggio dei pagamenti effettuati per il tramite dei suddetti strumenti;
- registrare e/o conservare documentazione attestante le transazioni ed i pagamenti effettuati in nome e per conto della Società attraverso i suddetti strumenti;
- 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 "rimborso spese vive") e/o autorizzativa in base al sistema di poteri e deleghe in essere.

Inoltre, con riferimento ai comportamenti che i soggetti interessati devono o non devono porre in essere, **è <u>severamente vietato:</u>**

- 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.

Attività n. 3 Processo di verifica delle attività aziendali svolte tramite l'utilizzo di apparecchiature, dispositivi e/o programmi informatici aziendali

- predisposizione di adeguate misure di sicurezza di natura organizzativa, fisica e logistica, in modo da minimizzare il rischio degli accessi non autorizzati, di alterazione, di divulgazione, di perdita o distruzione delle risorse informatiche e che si pongono quale obiettivo quelli 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;
- utilizzare i dispositivi, programmi o apparecchiature informatiche assegnati esclusivamente per l'espletamento della propria attività;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informatici della Società, evitando che i terzi soggetti possano venirne a conoscenza;
- garantire la tracciabilità dei documenti prodotti al fine di effettuare qualsivoglia pagamento.

N.B.: **Con riferimento agli illeciti di cui al presente documento, la Società sta elaborando una procedura *ad hoc* per ogni attività sensibile indicata all'interno della presente Parte Speciale atta a definire con precisione i comportamenti che i soggetti responsabili devono porre in essere al fine di prevenire la commissione di uno dei reati-presupposto interessati. Inoltre, la Società sta predisponendo – a supporto di ogni singola procedura – una scheda di mappatura della suddetta attività sensibile, alla quale si rimanda integralmente.**