

MODELLO DI ORGANIZZAZIONE E DI GESTIONE

PARTE SPECIALE N. 10

ART. 25 OCTIES 1 D. LGS. 231/01

(IN TEMA DI DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI)

Documento:	<i>Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/01</i>		
Approvazione:	<i>Consiglio di Amministrazione</i>	Verbale riunione del:	<i>24/01/2024</i>
Revisione:			
Revisione:			

1. I reati in materia di strumenti di pagamento diversi dai contanti
2. I processi e le aree a rischio individuate
3. I presidi di controllo
4. Compiti dell'Organismo di Vigilanza e flussi informativi

1. **I REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI**

L'art. 25 *octies* 1 del D. Lgs. 231/01 - introdotto dall'art. 3, comma 1, del D. Lgs. 8 novembre 2021, n. 184 - indica, tra i reati presupposto per la responsabilità amministrativa delle società, i delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti e, in particolare, il reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter* c.p.); la 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.) e la frode informatica aggravata (art. 640 *ter* comma 2 c.p.)

Di seguito si passano ad analizzare le singole fattispecie criminose.

A. Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 *ter*¹ 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

¹ La previsione di una tutela penale delle carte di credito o pagamento e dei documenti equiparati ha costituito una delle misure approntate per prevenire il riciclaggio, perché incentiva il ricorso a strumenti alternativi al contante che consentono anche l'identificazione dell'autore delle transazioni (cfr. la sentenza della Corte Costituzionale n. 302/2000). Da un lato, infatti, la notevole diffusione dei sistemi informatici e di intermediazione finanziaria e dall'altro l'esigenza di assicurare, *erga omnes*, la tutela della buona fede e la certezza dei rapporti economici con essi soddisfatti hanno indotto il legislatore a sanzionare fattispecie che non erano punite o non lo erano adeguatamente rispetto al disvalore del fatto. La norma incriminatrice originariamente è stata introdotta con l'art. 12 d.l. 3 maggio 1991, n. 143 conv. con modificazioni in Legge 5 luglio 1991, n. 197 ("Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e per prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio") per integrare le disposizioni relative alla ricettazione, al falso e all'emissione di assegni senza autorizzazione del trattario e senza provvista. Successivamente è stata riprodotta dall'art. 55, comma 9 d.lgs. 21 novembre 2007, n. 231 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminali e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e, a seguito del d.lgs. 25 maggio 2017, n. 90 è trasmigrata con immutata formulazione nel nuovo art. 55, comma 5, d.lgs. n. 231/2007. La giurisprudenza in diverse pronunce ha evidenziato la continuità normativa tra la fattispecie di cui all'art. 12 d.l. n. 143/1991 e quella di cui all'art. 55 d.lgs. n. 231/2007 (cfr. Corte di Cassazione, II Sezione Penale, sentenza n. 24527/2009).

In seguito il D.lgs. del 1° marzo 2018, n. 21 contenente le "Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'art. 1, comma 85, lett. q), l. 23 giugno 2017, n. 103" ha sancito da un lato l'abrogazione del comma 5 del summenzionato art. 55, dall'altro, all'art. 4 l'introduzione dell'art. 493 *ter* all'interno del codice penale. Il legislatore delegato, infatti, ha ritenuta la norma eliminata del tutto estranea al testo normativo dedicato alla prevenzione del riciclaggio e, pertanto, da inserire nel codice penale (cfr. la Relazione governativa allo Schema di D.Lgs. n. 21/2018).

acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

L'art. 493 *ter* può essere qualificato una “disposizione a più norme” perché scandisce tre autonome incriminazioni di forme diverse di abuso di carte di pagamento:

- 1) nell'indebita utilizzazione, da parte di chi non ne è titolare, di carte di credito o pagamento o di qualsiasi altro documento analogo che abiliti al prelievo di contante, all'acquisto di beni o alla prestazione di servizi, o comunque di ogni altro strumento di pagamento diverso dai contanti;
- 2) nella falsificazione o nell'alterazione dei medesimi documenti o strumenti;
- 3) nel possesso, nella cessione o nell'acquisizione degli strumenti e dei documenti descritti, ove di provenienza illecita, o di ordini di pagamento prodotti con essi.

Oggetto materiale della fattispecie sono, quindi, le carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi od ordini di pagamento prodotti con documenti di provenienza illecita o comunque falsificati o alterati o comunque ogni altro strumento di pagamento diverso dai contanti.

Sono carte di credito o di pagamento le tessere munite di una banda magnetica e/o di microcircuiti sui quali sono impressi i dati di identificazione del titolare, i limiti e le modalità di utilizzo, nonché gli estremi del rapporto con l'azienda o l'ente che ha rilasciato il documento abilitante alla fruizione dei servizi (bancomat, carte di credito, carte prepagate).

L'espressione “*altri documenti con analogo funzione*” è stata riportata per ricomprendere nella disposizione normativa ogni ulteriore supporto che presenta la medesima utilità economica. In particolare, a titolo esemplificativo, la giurisprudenza ha individuato, tra i documenti analoghi negli strumenti di pagamento: la tessera a banda magnetica a scalare per il pagamento del pedaggio autostradale “viacard”, la tessera carburanti, la smart card per il noleggio di film in dvd, le tessere telefoniche prepagate (in quanto abilitano il titolare-possessore all'accesso di servizi della rete telefonica) e i vaglia postali veloci (in quanto sono caratterizzati dall'“imprimatur” di un codice alfanumerico che attribuisce solo a chi conosce la sequenza dei numeri la possibilità di prelevare il denaro, sia pure per il tramite dell'operatore allo sportello).

Al fine di ampliare l'ambito di applicazione dei delitti di cui all'art. 493 *ter* c.p., l'art. 2 del D. Lgs. n. 184 del 2021 ha incluso tra gli oggetti materiali anche tutti gli strumenti di pagamento diversi dai contanti, individuati con la definizione fornita dall'art. 1, comma 1, lett. a) del D. Lgs. n. 184 del 2021, ovvero ogni “*dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a 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*”. Sempre l'art. 1 chiarisce alla lett. b) che per “*dispositivo, oggetto o record protetto*” s'intende un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma e alla lett. c) che “*mezzo di scambio digitale*” è sia qualsiasi moneta elettronica così come definita all'art. 1, comma 2, lett. h-ter, del D.Lgs. n. 385 del 1993, sia la valuta virtuale (ovvero, ai sensi della lett. c) “*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da*

persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente”.

Come sopra detto, le condotte descritte nella norma consistono:

- a) nell'utilizzare indebitamente, cioè senza esserne titolare, carte di credito o di pagamento o 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 al fine di trarne profitto per sé o per altri.

Nello specifico, la condotta consiste nel disporre o nel servirsi delle predette carte o documenti o strumenti di pagamento alternativi ai contanti conformemente alla loro normale destinazione per ricavarne un vantaggio. Il loro materiale possesso non costituisce un presupposto necessario per l'integrazione del reato: è sufficiente, infatti, che l'agente, attraverso l'immissione dei dati ricognitivi e operativi di una valida carta di credito altrui di cui non ha la materiale disponibilità, effettui delle transazioni non autorizzate dal titolare. L'utilizzo della carta è indebito quando manca il consenso del titolare o sono violate le prescrizioni e le modalità d'impiego stabilite dall'emittente o dall'ente erogatore. Il titolare, infatti, ha titolo valido per l'utilizzazione del documento solo se perdura il rapporto contrattuale che ha dato luogo alla concessione della carta e ne ha autorizzato l'uso. L'uso indebito non deve essere confuso con quello illegale e, quindi, *contra legem*: il primo, infatti, va ricondotto al concetto più ristretto di illecito civile per violazione delle regole convenzionali intervenute tra le parti, in quanto il significato etimologico e tecnico è quello di prestazione ingiusta e non dovuta. Uso indebito è, quindi, quello che, *contra pactum atque condicionem*, viola la disciplina convenzionale del rapporto tra ente di intermediazione finanziaria e utente. Al fine di individuare la sfera applicativa della norma la giurisprudenza ha chiarito che la titolarità della carta deve essere sostanziale, legale e attuale e non formale, ovvero derivante dall'intestazione o dal mero possesso di essa. Di conseguenza il soggetto, apparente titolare della carta di credito, commette il delitto se utilizza una carta il cui contratto è estinto o è stato sospeso per qualsiasi causa. Non essendo, infatti, più titolare del rapporto contrattuale con l'emittente, non ha più il diritto a servirsene. In tale ipotesi è necessario, però, sotto il profilo soggettivo, che l'agente sia consapevole del recesso e, quindi, che vi sia stata la comunicazione all'utente della revoca dell'autorizzazione ad usare la carta di credito. Per perimetrare l'ambito di applicazione della norma la giurisprudenza ha distinto l'ipotesi in cui la carta di credito è nominativa da quella in cui è al portatore. Nel primo caso l'indebito utilizzo sussiste tutte le volte che la carta sia usata da chi non ne sia titolare (salvo il consenso dell'avente diritto); mentre, nel secondo (ad es. della carta ricaricabile Viacard) il reato si realizza quando il soggetto ha fatto uso della carta con la consapevolezza di non esserne titolare.

Ai fini della consumazione del delitto occorre, inoltre, che l'agente usi la carta o il documento indebitamente «*per trarne profitto per sé o per altri*» e non è necessario che quest'ultimo si sia effettivamente concretizzato.

- b) nel falsificare o alterare carte di credito o di pagamento o 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, al fine di trarne profitto per sé o per altri.

Nello specifico, la falsificazione consiste nella materiale creazione, da parte di un soggetto non legalmente autorizzato, di una nuova carta di credito “artefatta” (o di un documento o di uno strumento di pagamento alternativo ai contanti fasullo) solo apparentemente riconducibile all'istituto emittente, ma in realtà priva di qualsiasi collegamento negoziale con quest'ultimo e tale da far apparire al lettore magnetico che essa proviene dall'emittente ed è utilizzata dal soggetto legittimato.

L'alterazione, invece, presuppone l'esistenza di una carta regolarmente creata dall'emittente e si concretizza nella sua manipolazione artificiosa attraverso la modificazione di alcuni dati rilevanti quali l'intestazione, la data di scadenza, il nome del titolare, la banda magnetica o dei dati in essa inseriti che permettono l'accesso ai servizi o, infine, dei codici per consentirne un uso diverso per qualità e quantità rispetto a quello previsto dall'ente emittente (limiti di spesa o di prelievo).

Anche in questa ipotesi non occorre che il profitto si sia effettivamente concretizzato.

- c) nel possedere, cedere o acquistare tali strumenti di pagamento diverso dai contanti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi, al fine di trarne profitto per sé o per altri.

Nello specifico, per possesso si intende la concreta disponibilità, anche temporanea e a qualsiasi titolo, della carta o del documento analogo o dello strumento di pagamento diverso dai contanti costituisce il presupposto delle condotte di cessione e acquisizione. Il concetto di possesso deve essere inteso in senso penalistico, ovvero come autonoma disponibilità della *res* accompagnata dall'*animus rem sibi habendi*, cioè dall'animo di tenere la cosa presso di sé.

L'acquisizione si sostanzia nel conseguimento del possesso della carta o del documento o dello strumento di pagamento diverso dai contanti e indica il rendersi destinatario, come acquirente, del suo trasferimento (e fuori dall'ipotesi di mero rinvenimento casuale), mentre la cessione nella sua alienazione. Le condotte di cessione o acquisizione, pertanto, ricomprendono tutte le possibili modalità di trasferimento a terzi delle carte, dei documenti e degli strumenti di pagamento diversi dai contanti, ivi comprese quelle a titolo gratuito o a titolo oneroso, perché l'area di operatività della norma non è limitata a quelle in cui il trasferimento avvenga contro prezzo e si inquadri, pertanto, in un negozio, pur illecito, di compravendita. La provenienza illecita, infine, postula che il possesso della carta di credito o del documento analogo o dello strumento di pagamento diverso dai contanti debba derivare da un illecito civile, amministrativo o anche penale, ma di natura contravvenzionale perché nell'ipotesi in cui sia ricollegabile ad un delitto si configura il reato di ricettazione di cui all'art. 648 c.p. Anche in riferimento a queste fattispecie ai fini della loro consumazione non è necessaria la realizzazione del profitto.

I delitti previsti dall'art. 493 *ter* sono puniti a titolo di dolo specifico, consistente nella coscienza e volontà di utilizzare la carta di pagamento o il documento o lo strumento di pagamento diverso dai contanti (nel primo reato) e di falsificare o alterare (nel secondo) o possedere, cedere o acquistare tali strumenti di pagamento o documenti (nel terzo) al fine di trarne profitto per sé o per altri.

Sanzioni pecuniarie ex. D. Lgs. 231/01: da 300 a 800 quote. Ai sensi dell'art. 12 del D.lgs. n. 231/2001, la sanzione è diminuita della metà, se *i)* l'autore del reato ha commesso il fatto nel

prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; ii) il danno patrimoniale cagionato è di particolare tenuità; è diminuita da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado l'ente i) ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; ii) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della stessa specie di quello verificatosi. Se concorrono entrambe le condizioni di cui sopra la sanzione è ridotta dalla metà a due terzi.

Sanzioni interdittive ex D. Lgs. 231/01: ai sensi dell'art. 25 *octies* 1 comma 3 e dell'art. 9 comma 2 del D.lgs. n. 231/2001, sono previste le seguenti sanzioni interdittive per una durata non inferiore a tre mesi e non superiore a due anni:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi

B. La 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.

La condotta costitutiva del reato consiste nel produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri l'oggetto materiale del reato – vale a dire sia apparecchiature che dispositivi informatici (hardware, ad es. chiavi USB, cd-rom, dvd, floppy disk, hard disk esterni, ecc.) sia programmi informatici (cosiddetti software) la cui finalità è quella di commettere reati riguardanti strumenti di pagamento alternativi ai contanti e si caratterizza per essere finalizzata a consentire l'uso o a permettere l'utilizzo da parte di altri delle apparecchiature, dispositivi o programmi informatici predisposti o adattati proprio per commettere reati riguardanti strumenti di pagamento diversi dai contanti.

Il delitto previsto dall'art. 493 *quater* è punito a titolo di dolo specifico, consistente nella coscienza e volontà di porre in essere le condotte descritte dalla norma (produrre, importare, ecc.) al fine di utilizzare o di consentire ad altri l'uso di apparecchiature, dispositivi o programmi informatici realizzati o adattati per commettere reati riguardanti strumenti di pagamento diversi dai contanti.

Sanzioni pecuniarie ex D. Lgs. 231/01: sino a 500 quote. Ai sensi dell'art. 12 del D.lgs. n. 231/2001, la sanzione è diminuita della metà, se *i)* l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; *ii)* il danno patrimoniale cagionato è di particolare tenuità; è diminuita da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado l'ente *i)* ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *ii)* è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della stessa specie di quello verificatosi. Se concorrono entrambe le condizioni di cui sopra la sanzione è ridotta dalla metà a due terzi.

Sanzioni interdittive ex D. Lgs. 231/01: ai sensi dell'art. 25 *octies* 1 comma 3 e dell'art. 9 comma 2 del D.lgs. n. 231/2001, sono previste le seguenti sanzioni interdittive per una durata non inferiore a tre mesi e non superiore a due anni:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi.

C. Frode informatica (art. 640 *ter* primo e secondo comma c.p.)

[I]. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

[II]. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se [...] il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

Il delitto di frode informatica, previsto dall'art. 640 *ter* c.p., è stato introdotto nel codice penale con l'art. 10 Legge 23 dicembre 1993, n. 547, recante modifiche al codice penale e di procedura in tema di criminalità informatica; la suddetta fattispecie incriminatrice è rivolta specificamente alla repressione delle frodi informatiche, cioè di quelle condotte attuate mediante l'utilizzazione di elaboratori elettronici, estendendosi la tutela penale a quelle attività truffaldine che, per

avere quale oggetto materiale uno strumento elettronico e non una persona fisica, non potevano rientrare nella fattispecie generale della truffa di cui all'art. 640, stante, appunto, la mancanza del soggetto ingannato. È stata, quindi, introdotta una nuova figura di reato avente carattere plurioffensivo, nel quale accanto alla necessità di salvaguardare il patrimonio del soggetto passivo, da identificare nel titolare del sistema informatico o telematico, si è ritenuto di offrire tutela penale anche alla sicurezza del sistema informatico stesso ed all'integrità dei dati in esso contenuti. La fattispecie, quindi, prevede due condotte alternative di realizzazione del reato: da un lato l'alterazione di un sistema informatico o telematico, attuabile con le modalità più diverse, attraverso la quale il sistema viene modificato o manipolato, quindi distratto dai suoi schemi predefiniti, in vista del perseguimento da parte dell'agente di un ingiusto profitto con altrui danno; da un altro lato l'intervento, con qualsiasi modalità attuativa, sui dati, le informazioni o i programmi contenuti nel sistema effettuato in modo da realizzare un ingiusto profitto con altrui danno.

Viene definito sistema informatico, secondo la ricorrente espressione utilizzata nella Legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti *computer's crimes*, un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate — per mezzo di un'attività di «codificazione» e «decodificazione» — dalla «registrazione» o «memorizzazione», per mezzo di impulsi elettronici, su supporti adeguati, di «dati», cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Per l'integrazione del reato, dal punto di vista soggettivo, è necessario il dolo generico, vale a dire la coscienza e volontà di alterare il sistema.

Il delitto è aggravato in caso di realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale.

Sanzioni pecuniarie ex D. Lgs. 231/01: sino a 500 quote. Ai sensi dell'art. 12 del D.lgs. n. 231/2001, la sanzione è diminuita della metà, se *i)* l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; *ii)* il danno patrimoniale cagionato è di particolare tenuità; è diminuita da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado l'ente *i)* ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *ii)* è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della stessa specie di quello verificatosi. Se concorrono entrambe le condizioni di cui sopra la sanzione è ridotta dalla metà a due terzi;

Sanzioni interdittive ex D. Lgs. 231/01: ai sensi dell'art. 25 *octies* 1 comma 3 e dell'art. 9 comma 2 del D.lgs. n. 231/2001, sono previste le seguenti sanzioni interdittive per una durata non inferiore a tre mesi e non superiore a due anni:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi

D. TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 512 BIS C.P.)

[1]. Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter, è punito con la reclusione da due a sei anni.

Tale reato è quello già previsto dall'art. 12-*quinques* comma 1 d.l. n. 306/1992 "Modifiche urgenti al nuovo codice di procedura penale e provvedimenti di contrasto alla criminalità mafiosa" convertito con modificazioni nella l. n. 356/1992 e punisce colui che attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando o al fine di agevolare la commissione del delitto di ricettazione, riciclaggio o impiego di denaro, beni o utilità di provenienza illecita.

Poiché il d.lgs. n. 21/2018, ha disposto l'abrogazione dell'art. 12-*quinques* e ha contestualmente disposto l'inserimento della medesima fattispecie di reato, con la medesima disciplina, nel nuovo art. 512-bis c.p., il fenomeno successorio che si è verificato risulta caratterizzato da una evidente continuità normativa tra l'ipotesi formalmente abrogata e l'analoga previsione introdotta all'interno del codice penale.

La norma ha portata generale in quanto il soggetto attivo può essere chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità.

Il reato di cui all'art. 512 bis c.p. è configurabile in capo all'autore del delitto presupposto, il quale attribuisca fittiziamente ad altri la titolarità o la disponibilità di denaro, beni o altre utilità, di cui rimanga effettivamente "dominus", al fine di agevolare una successiva circolazione nel tessuto finanziario, economico e produttivo, poiché la disposizione di cui sopra consente di perseguire anche i fatti di autoricettazione, riciclaggio o reimpiego. Il delitto può essere commesso anche da chi non sia ancora sottoposto a misura di prevenzione e anche prima che il relativo procedimento sia iniziato, occorrendo solo, per la configurabilità del dolo specifico previsto dalla norma, che l'interessato possa fondatamente presumerne l'avvio; pertanto, non occorre la preventiva emanazione delle misure di prevenzione, né la pendenza del relativo procedimento, bastando soltanto che l'autore ne possa temere l'instaurazione.

Quando l'interposto si rende fittiziamente titolare di beni o di utilità al fine di eludere misure ablatorie o le norme in materia di prevenzione patrimoniale o di contrabbando o al fine di agevolare la commissione dei reati di ricettazione, riciclaggio e di rimpiego di beni di provenienza illecita, risponde a titolo di concorso [ex art. 110 c.p.](#), del medesimo reato ascritto a colui che ha operato la fittizia attribuzione, in quanto, con la sua condotta cosciente e volontaria, contribuisce alla lesione dell'interesse protetto dalla norma incriminatrice.

La giurisprudenza ha specificato che, se da un lato i termini “titolarità” e “disponibilità” impongono di comprendere nella previsione normativa non solo le situazioni del proprietario o del possessore ma anche quelle nelle quali il soggetto venga comunque a trovarsi in un rapporto di signoria con il bene; dall'altro lato, impongono altresì di considerare ogni meccanismo che realizzi la fittizia attribuzione consentendo al soggetto incriminato di mantenere il proprio rapporto con il bene.

La norma sanziona, pertanto, tutte quelle condotte che realizzano di fatto, nelle modalità più disparate, una situazione di apparenza, con la separazione tra colui o coloro che hanno la titolarità effettiva di denaro o utilità e colui o coloro che, in base ad una fittizia attribuzione, ne risultano formalmente titolari o disponenti.

Tale fattispecie si caratterizza, quindi, per la consapevole determinazione, realizzata in qualsiasi forma, di una situazione di difformità tra titolarità formale, meramente apparente, e titolarità di fatto di un determinato compendio patrimoniale, qualificata dalla specifica finalizzazione fraudolenta normativamente descritta. Per questa sua caratteristica, risulta irrilevante che il provvedimento di prevenzione non sia ancora disposto, poiché - alla luce dell'interesse giuridico sotteso al reato - conserva indubbiamente interesse penale la cessione dei beni disposta proprio al fine di sottrarli all'effetto ablativo della misura.

2. I PROCESSI E LE AREE A RISCHIO INDIVIDUATE

Con riferimento specifico ai reati societari, ai fini della presente Parte Speciale i processi sensibili e le aree a rischio sono i seguenti.

- a. Flussi Finanziari
- b. Acquisti di beni, servizi e consulenze
- c. Amministrazione, Finanza e Controllo.

3. I PRESIDI DI CONTROLLO

L'obiettivo delle procedure e dei presidi di seguito indicati è garantire che tutti i soggetti, a vario titolo coinvolti nei processi sopra elencati, mantengano condotte conformi alla legge ed alla politica aziendale così da prevenire la commissione dei reati indicati nel precedente paragrafo 1.

Al fine di prevenire ed impedire il verificarsi dei Delitti in materia di Strumenti di pagamento diversi dai contanti, i Destinatari del Modello coinvolti nello svolgimento delle Attività Sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- astenersi dal porre in essere o in qualsiasi modo contribuire alla realizzazione delle fattispecie di cui all'art. 25 *octies* 1 del D.Lgs. 231/01;
- monitorare e tracciare i flussi monetari e finanziari in entrata ed in uscita dalla Società;
- individuare i Responsabili aziendali che, in ragione dell'attività svolta, dispongono di carte di credito aziendali, nonché definizione dei criteri di assegnazione e modalità di utilizzo delle stesse;

- astenersi da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni dei dati aziendali e di terzi, ed in particolare assicurarsi, nei casi in cui si debba allontanare dalla postazione di lavoro, di non lasciare incustoditi i documenti contenenti dati relativi a strumenti di pagamento con i propri codici di accesso, accertarsi di avere spento il computer e tutte le periferiche al termine del proprio turno di lavoro;
- utilizzare in modo appropriato e confacente agli scopi aziendali le carte di credito, le carte prepagate, e/o altri strumenti di pagamento della Cooperativa, avendo cura di custodire e proteggere i relativi dati;
- assicurare che l'intermediario scelto garantisca elevati livelli di sicurezza delle informazioni gestite, nonché soddisfi tutti i più alti requisiti normativi in materia di pagamento elettronici;
- conservare la documentazione a supporto, adottando tutte le misure di sicurezza, fisica e logica necessarie;
- favorire la diffusione all'interno della Società di una cultura improntata alla compliance e alla prevenzione del rischio informatico e telematico, sensibilizzando tutti sulle tematiche per una valutazione preventiva di rischi.

Inoltre, ai Destinatari del Modello è fatto divieto in particolare di:

- archiviare, duplicare o utilizzare impropriamente documenti che al loro interno contengono dati di carte di pagamento, ovvero astenersi dall'attuare qualsiasi condotta diretta a neutralizzare o aggirare le protezioni del sistema informatico aziendale o altrui;
- non rispettare i principi e le indicazioni contenute nelle procedure specifiche adottate dalla Società.

Con riguardo ai reati in materia di Strumenti di pagamento diversi dai contanti:

PROCESSO O AREA A RISCHIO	PRESIDI DI CONTROLLO ESISTENTI
Flussi Finanziari	Codice etico Procedura gestione e controllo tesoreria Da amministrazione a servizi Procedura sistema informativo Definizione organizzazione e gestione
Acquisti di beni, servizi e consulenze	Codice etico Procedura acquisti Procedura sistema informativo Procedura Gestione delle consulenze e degli incarichi professionali_07.22 Da amministrazione a servizi Approvvigionamenti

Amministrazione, Finanza e Controllo.	Codice etico Procedura gestione e controllo tesoreria Da amministrazione a servizi Procedura sistema informativo Definizione organizzazione e gestione
---------------------------------------	--

4. COMPITI DELL'ORGANISMO DI VIGILANZA E FLUSSI INFORMATIVI

Fermo restando quanto previsto nella Parte Generale del Modello, e salvo il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, è compito dell'O.d.V.:

- effettuare verifiche periodiche sul rispetto della presente parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25 *octies* 1 del Decreto, attraverso controlli a campione sulle citate aree a rischio reato;
- vigilare sull'effettiva applicazione del Modello e rilevare le violazioni comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- monitorare l'efficacia delle procedure interne volte a prevenire la commissione dei reati disciplinati nella presente Parte Speciale;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale in ordine a presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività del medesimo.

Per l'adempimento di tali compiti, è necessario che sia implementato ed attuato un costante scambio di informazioni tra i destinatari del Modello e l'Organismo di Vigilanza.

A tal fine, l'O.d.V. viene informato semestralmente dalle funzioni aziendali interessate (tramite apposite relazioni) in merito alle attività sensibili e, immediatamente, in caso di commissione di reati o di condotte potenzialmente idonee ad integrare le fattispecie di reato rilevanti ai fini della presente Parte Speciale, nonché nell'ipotesi di:

- violazioni, accertate o sospette, del Modello o delle procedure ad esso correlate o degli elementi che lo compongono;
- condotte e/o pratiche non in linea con le disposizioni del Codice Etico adottato dall'ente.

La funzione preposta deve dare immediata comunicazione all'Organismo di Vigilanza di ogni deroga alle procedure di processo decisa in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.

L'Organismo di Vigilanza avrà accesso a tutta la documentazione aziendale.

I Responsabili delle Funzioni devono, inoltre, comunicare, per quanto di competenza e con periodicità definita dei campioni di documentazione relativa alla fatturazione e alla gestione monetaria. L'Organismo di Vigilanza può chiedere eventuali integrazioni documentali sul punto.

Eventuali modifiche o integrazioni dei flussi informativi che saranno ritenuti utili per il corretto esercizio della propria attività sono rimesse alla competenza dell'Organismo di Vigilanza.

A sua volta, l'Organismo di Vigilanza deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati societari, al Consiglio di Amministrazione, secondo i termini indicati nella Parte Generale del Modello e nel Regolamento di cui l'Organismo di Vigilanza vorrà dotarsi.