Li.Bo S.r.l.

Aggiornamento del Modello ex D.lgs. n. 231/2001

(da intendersi quale parte integrante e sostanziale del Modello 231 adottato)

Art. 493 quater c.p.

"Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"

Art. 640 ter c.p.

"Frode informatica"

Approvato dall'Amministratore Unico in data 22/05/2023

In data 29 novembre 2021 è stato pubblicato in Gazzetta Ufficiale il D.Lgs. 8 novembre 2021, n. 184 in attuazione della legge delega 22 aprile 2021, n. 53 recante *"Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea".*

In particolare, tale intervento si è reso necessario per adeguare la normativa nazionale alla direttiva 17 aprile 2019, n. 2019/713/UE del Parlamento europeo e del Consiglio, dedicata alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. Il decreto, composto di sei articoli, si pone l'obiettivo di aggiornare gli strumenti di lotta alle predette frodi, modificando alcuni articoli del codice penale, aggiornando il catalogo dei reati presupposto della responsabilità da reato dell'ente e rafforzando gli strumenti di cooperazione con le istituzioni europee (D.Lgs. 8 novembre 2021, n. 184 – G.U. 29 novembre 2021, n. 284, Suppl. ord. n. 40).

Art. 493 quater c.p. "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"

L'art. 2 del d. lgs. n. 184/2021, introduce anche una nuova fattispecie all'interno del c.p., all'art. 493-quater, rubricato *"**Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti**".*

Tale fattispecie punisce con la reclusione fino a due anni e con la multa fino a 1000 euro, salvo che il fatto costituisca più grave reato, chiunque produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sè o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti, o sono specificamente adattati al medesimo scopo.

Trattasi di un reato comune, come indiziato dall'uso del pronome "chiunque", punito a titolo di dolo specifico, in quanto le condotte suddette assumono rilevanza penale quando siano poste in essere con il fine specifico di far uso degli strumenti indicati o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti.

La disposizione si completa con la previsione, al secondo comma, della confisca

obbligatoria, in caso di condanna o patteggiamento, delle apparecchiature, dei dispositivi o dei programmi informatici utilizzati per commettere reati riguardanti strumenti di pagamento diversi dai contanti, nonchè della confisca del profitto o del prodotto del reato ovvero, quando quest'ultima non sia possibile, della confisca per equivalente di beni, somme di denaro e altre utilità di cui il reo abbia la disponibilità per un valore corrispondente al profitto o prodotto.

Come emerge già dalla rubrica, si tratta di un **reato prodromico** alla commissione di ulteriori reati concernenti mezzi di pagamento diversi dai contanti; la norma – che rappresenta l'attuazione dell'art. 7 della già citata Dir. 2019/713/UE – incrimina infatti la produzione e varie altre condotte di trasferimento di "apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere [reati riguardanti gli strumenti di pagamento diversi dai contanti] o sono specificamente adattati al medesimo scopo".

Un'ulteriore questione interpretativa che la norma potrebbe porre riguarda la **corretta individuazione della condotta penalmente rilevante**: il testo della norma, come sopra già detto, fa riferimento a colui che *"produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o ad altri"* gli oggetti o i software finalizzati alla commissione di reati in materia di mezzi di pagamento; **non è menzionato, invece, il mero possesso** di tali beni materiali o immateriali, che invece sembrerebbe essere oggetto della norma alla luce della rubrica. Il fatto di punire il mero "procurare a sé" l'oggetto materiale del reato, poi, non parrebbe sufficiente a consentire la punizione del mero possesso, sulla base dell'assunto per cui "chi detiene qualcosa se lo deve essere in qualche modo procurato": è necessario, infatti, che la condotta sia colorata dal "fine di farne uso o di consentirne ad altri l'uso nella commissione di reati", fine che deve sussistere al momento in cui il soggetto si è procurato il bene in questione, posto che quella – e solo quella – è la condotta considerata dalla norma.

Art. 640 ter c.p."Frode informatica"

Oltre alla modifica all'art. 493-ter e all'introduzione dell'art. 493-quater nel codice, il decreto in esame contiene **l'art. 640-ter c.p., il cui secondo comma, è stato emendato con l'inserimento di un'ulteriore ipotesi aggravante**, che ricorre quando il fatto "produce un trasferimento di denaro, di valore monetario o di valuta virtuale".

Tale aggravante determina l'equiparazione della pena tra la frode informatica e l'indebito utilizzo e la falsificazione di mezzi di pagamento, equiparazione che pare ragionevole se si considera che la giurisprudenza riconduce alla fattispecie di cui all'art. 493-ter l'indebito utilizzo di carta di credito per effettuare pagamenti o prelievi di denaro contante, mentre riconduce all'art. 640-ter la non meno grave ipotesi di utilizzo indebito dei codici della medesima carta per effettuare operazioni online.

Si rammenta che tale delitto era stato già introdotto nel 2001, quale reato presupposto della versione originaria del Decreto 231 – esattamente nell'art. 24 – ma con una rilevanza ridotta, ovvero solo se commesso «in danno dello Stato o di altro ente pubblico» (ipotesi di danno che è stato poi esteso all' "Unione Europea" con il D.Lgs. 75/2020). In altri termini, non era – e continua a rimanere tale – giuridicamente punibile ex D.Lgs. 231/2001 una eventuale frode informatica in danno di un privato.

Con il D.Lgs. 184/2021 il reato di frode informatica ex art. 640 ter c.p. viene re-introdotto nel D.Lgs. 231/2001 attraverso il nuovo art. 25 octies.

L'art. 3 del D.Lgs. 184/2021, non interviene minimamente sull'art. 24 del D.Lgs. 231/2001, né dispone alcuna estensione applicativa del richiamato reato presupposto. In conclusione, la frode informatica rimane presente nel D.Lgs. 231/2001 nelle sue due distinte ed autonome "versioni":

nell'art. 24, quale reato punibile nella sua previsione integrale, ma solo se commesso in danno dello Stato o di altro ente pubblico o dell'Unione Europea;

nell'art. 25 octies, quale reato punibile anche nei confronti di un privato, ma a condizione che sia prospettabile l'aggravante di un fatto illecito che abbia prodotto un trasferimento di denaro, di valore monetario o di valuta virtuale.

Aree di rischio

Per ascrivere all'ente la responsabilità amministrativa da illecito è necessario che il reato sia commesso nell'interesse o vantaggio dell'ente stesso.

Le fattispecie in argomento (art. 493 quater c.p. e 640 ter c.p.) di cui all'art. 25 octies del D.lgs. 231/01, attengono all'**Area di gestione, controllo e monitoraggio, dei flussi patrimoniali e finanziari della società, che afferiscono alla gestione, diretta o indiretta, degli strumenti di pagamento (in entrata o in uscita) e dei movimenti monetari.**

Pur tuttavia, si rileva che la disposizione di cui all'art. 25-octies trova applicazione in misura prevalente con riferimento a quelle realtà imprenditoriali aventi come *core*

business la conservazione e la gestione di capitali altrui (istituti di credito, società di intermediazione finanziaria o di gestione di fondi di investimento) o che si occupino della realizzazione di apparecchiature, dispositivi e sistemi informatici che vengano in contatto con strumenti di pagamento diversi dai contanti, aventi in ragione dell'attività svolta la disponibilità di dati e informazioni che consentano l'utilizzo di tali capitali.

Criteri efficaci di prevenzione dei reati

E' fatto onere alla Società di:

1) implementare le misure tecniche, operative e organizzative che assicurino un alto livello di protezione e sicurezza di dati onde evitare la perpetrazione di illeciti di frode e falsificazione degli strumenti di pagamento non rispondenti ad obiettivi che la Società ha inteso perseguire nello svolgimento della propria attività economica; in tal senso si invita la Società a dotarsi della Certificazione ai sensi della norma UNI ISO/IEC 27001:2017 *(Sistema di Gestione della Sicurezza delle Informazioni)*;

2) garantire un'adeguata politica di sicurezza informatica ai lavoratori dipendenti addetti alle mansioni di gestione degli strumenti di pagamento e delle movimentazioni monetarie della società, prevedendo appositi corsi di formazione ed informazione, ed aggiornamenti;

3) è fatto divieto assoluto alterare - in qualsiasi modo - il funzionamento di un sistema informatico o telematico, al fine di conseguire per sé o per altri un ingiusto profitto con altrui danno; (*per alterazione deve intendersi ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software);*

4) è fatto, altresì, divieto assoluto intervenire - senza diritto - con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti finalizzato a conseguire per sé o per altri un ingiusto profitto con altrui danno; (*per intervento deve intendersi ogni illecita condotta intrusiva ma non alterativa del sistema informatico o telematico).*