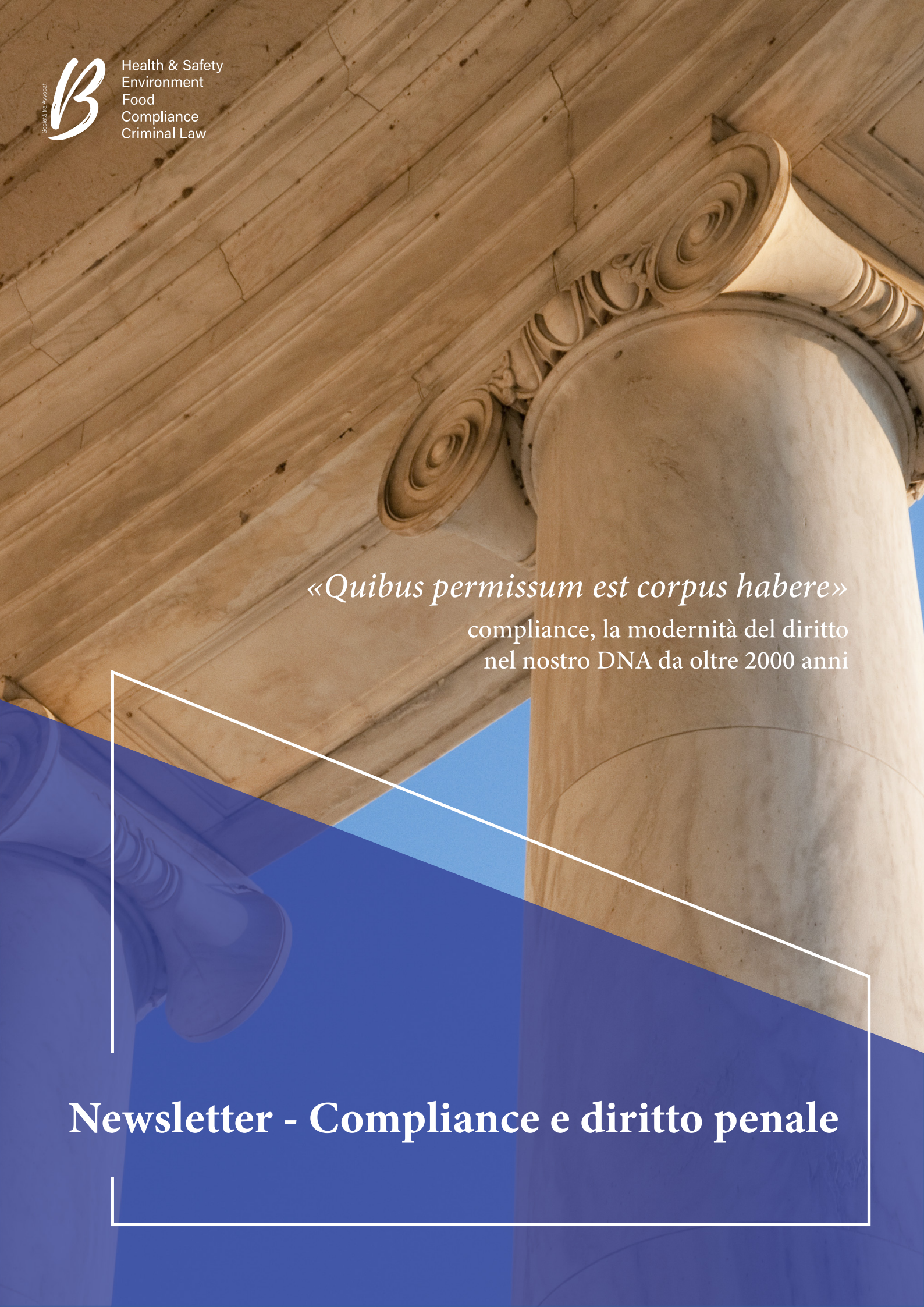
Società tra Avvocati

Health & Safety
Environment
Food
Compliance
Criminal Law



«Quibus permissum est corpus habere»

compliance, la modernità del diritto
nel nostro DNA da oltre 2000 anni

Newsletter - Compliance e diritto penale

Società tra Avvocati
Health & Safety
Environment
Food
Compliance
Criminal Law

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

NEWSLETTER COMPLIANCE E DIRITTO PENALE

Innovazioni penali della nuova legge europea

Sommario

1. Introduzione 2

2. Diritti informatici: estesa l'area del penalmente rilevante 2

3. Il nuovo volto dei market abuse 5

4. I riflessi delle modifiche legislative sulla responsabilità legislativa da reato *ex* D.Lgs. n. 231 del 2001 9

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

1. Introduzione

Il 1° febbraio 2022 è entrata in vigore la Legge 23 dicembre 2021, n. 238, recante «Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge europea 2019-2020»[1] (d'ora in avanti la "Legge europea") che, nel recepire l'acquis communautaire sulla scorta dei rilievi critici mossi dalla Commissione nell'ambito di tre distinte procedure di infrazione promosse nei confronti dell'Italia, ha apportato delle significative innovazioni al diritto penale sostanziale. Innovazioni che afferiscono ai:

- delitti informatici;
- reati di market abuse (abuso di informazioni privilegiate e manipolazione del mercato).
- riflessi delle modifiche legislative sulla responsabilità amministrativa da reato ex D.Lgs. n. 231 del 2001.

2. Diritti informatici: estesa l'area del penalmente rilevante

L'art. 19 della Legge europea[1] è intervenuta sulla disciplina penale in materia di contrasto alla criminalità informatica, modificando il corpo normativo degli art. 615-quater, 615-quinquies, 617, 617-bis, 617-quater e 617-quinquies c.p., con il dichiarato intento di uniformare l'ordinamento domestico alla Direttiva (UE) 2013/40 («relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio»), a margine delle censure formulate dalla Commissione europea nella procedura di infrazione n. 2019/2033.

Sul punto, merita dar conto che il Governo italiano, allo scadere del termine ultimo per il recepimento della Direttiva in parola da parte degli Stati membri (fissato per il 4 settembre 2015), aveva ritenuto l'ordinamento nazionale già compliant alle inedite previsioni eurounitarie – da qui il mancato recepimento della Direttiva stessa –, ancorando tale giudizio alla considerazione in base alla quale le Leggi n. 547 del 1993 e n. 48 del 2008 avevano consolidato nel tempo un presidio sanzionatorio e di enforcement non soltanto effettivo e completo, ma anche conforme alle indicazioni sovranazionali.

---

[1] *«Disposizioni per l'adeguamento alla direttiva n. 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. Procedura di infrazione n. 2019/2033».*

L'avvio della procedura di infrazione ha costituito, pertanto, l'occasione – invero, necessitata – per adeguare e corroborare la risposta punitiva dello Stato ai più recenti sviluppi del cybercrime; obiettivo, questo, perseguito dal legislatore del 2021 attraverso l'inasprimento delle cornici edittali delle norme incriminatrici e, soprattutto, mercè l'estensione dell'area del penalmente rilevante, quale diretto riflesso dell'ampliata descrizione delle condotte tipiche e dell'oggetto materiale dei delitti informatici.

In particolare, la novella ha modificato l'art. 615-quater c.p. (oggi rubricato «Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici e telematici»), per un verso, allargando le maglie applicative della fattispecie oggettiva sino a ricomprendervi le condotte di detenzione, produzione, messa a disposizione e installazione anche di apparati e strumenti finalizzati a consentire l'accesso ai sistemi di informazione e, per altro verso, innalzando la pena detentiva a due anni di reclusione.

A ben vedere, la nuova formulazione della norma in commento, al pari di quelle che verranno analizzate nel prosieguo, recepisce fedelmente l'obbligo posto in capo agli Stati membri dalla Direttiva (artt. 7 e 9) di adottare le misure necessarie affinché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione la messa a disposizione in altro modo di determinati strumenti informatici, orientati ad agevolare la commissione di un indebito accesso a sistemi di informazione, la interferenza illecita in un sistema o ai suoi dati, all'intercettazione illecita degli stessi, siano punibili come reato e, per di più, con una pena detentiva massima non inferiore ai due anni.

Contestualmente, è stato riformato il reato di cui all'art. 615-quinquies c.p. («Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telefonico»): l'intervento legislativo si è tradotto nell'ampliamento dell'area di precettività della fattispecie criminosa, che ora ingloba anche le condotte di abusiva detenzione, messa disposizione e installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere i sistemi informatici o telematici.

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

L'art. 26 della Legge europea è intervenuto, poi, sul delitto di cui all'art. 617 c.p. («Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche»), inasprendo il trattamento sanzionatorio dell'ipotesi base di cui al comma primo – che nella versione attuale contempla la pena della reclusione da un anno a sei mesi a cinque anni – e della fattispecie aggravata prevista dal comma terzo, da oggi punita con la reclusione da tre a otto anni.

La medesima ratio ha informato la novella del delitto di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, previsto e punito dall'art. 617-quater c.p.

Ben più incisiva si appalesa, invece, la modifica dell'art. 617-bis c.p. («Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche»), mercé la quale il legislatore nazionale ha demarcato la tipicità soggettiva dell'illecito, strutturandolo in chiave di reato a dolo specifico («al fine di prendere cognizione di una comunicazione o di una conversazione, telefonica o telegrafica, tra altre persone o comunque a lui non diretta, ovvero di impedirla o interromperla»), e, sul versante oggettivo, ha introdotto l'inedito riferimento alle condotte di detenzione, produzione, riproduzione, diffusione, importazione, comunicazione, consegna e messa a disposizione di apparati, strumenti, parti di apparati o di strumenti idonei a realizzare l'indebita attività di captazione delle conversazioni ovvero di interruzione delle stesse.

È evidente, in tal senso, l'effetto di armonizzazione della norma incriminatrice domestica con la previsione contenuta nell'art. 7 della Direttiva europea (v. supra).

Da ultimo, la modifica legislativa ha interessato l'art. 617-quinquies c.p. («Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche») – norma speculare all'art. 617-bis c.p. che anziona l'illecita intercettazione ed interferenza delle comunicazioni telefoniche –, ampliandone la fattispecie oggettiva, di guisa da far ricadere sotto il fuoco dell'incriminazione le condotte di detenzione, diffusione, produzione, riproduzione, diffusione, importazione, comunicazione, consegna e messa a disposizione di apparecchiature,

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

programmi, codici, parole o altri mezzi che manifestino attitudine a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (cfr. art. 7 Direttiva cit.). Al pari di quanto già osservato per l'art. 617-bis c.p., anche l'illecito in disamina risulta ora forgiato quale reato a dolo specifico, connotato dal fine di «intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle».

3. Il nuovo volto dei market abuse

La procedura d'infrazione n. 2019/2130, nell'ambito della quale la Commissione europea ha messo in mora l'Italia per il non corretto recepimento della Direttiva 2014/57/UE «relativa alle sanzioni penali in caso di abusi di mercato» (c.d. Direttiva MAD II), ha indotto il legislatore nazionale a uniformarsi alle censure mosse dall'organo esecutivo dell'Unione. A tale finalità risponde precipuamente l'art. 26 della Legge europea[2], laddove forgia un composito intervento novellatore sulla disciplina penale degli abusi di mercato di cui agli artt. 182 e ss. del D.Lgs. 24 febbraio 1998 n. 58 (T.U.F.), che si dispiega principaliter lungo cinque linee direttrici:

- modificare la morfologia e l'ambito di applicazione della disciplina sanzionatoria dell'abuso di informazioni privilegiate e di manipolazione del mercato, conferendo rilevanza a strumenti finanziari ulteriori rispetto a quelli già tipizzati dal previgente art. 182 T.U.F.;
- ampliare i casi di esenzione dalla predetta disciplina alle negoziazioni di valori mobiliari ovvero di strumenti collegati;
- introdurre una fattispecie criminosa autonoma e ad hoc per l'insider secondario;
- corroborare il trattamento sanzionatorio degli illeciti penali;
- limitare l'operatività della confisca al solo profitto dei reati di abuso del mercato, neutralizzando già sul piano astratto gli effetti della misura ablatoria verso il prodotto del reato ovvero i beni utilizzati per commetterlo.

[2] *«Disposizioni sanzionatorie in materia di abusi di mercato. Procedura d'infrazione n. 2019/2130».*

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

In prima battuta, non può trascurarsi che il novellato art. 182 T.U.F. («Ambito di applicazione») prevede ora che le disposizioni in materia di market abuse si applicano anche alle ipotesi illecite attinenti agli strumenti finanziari negoziati ovvero per i quali sia stata richiesta l'ammissione alla negoziazione in altre sedi rispetto a quelle già tipizzate (il riferimento implicito è ai sistemi multilaterali di negoziazione "MTF" e ai sistemi organizzati di negoziazione "OTF") e agli strumenti finanziari non negoziati in alcuna sede ("OTC"), in piena armonia con i dettami normativi della Direttiva MAD II (art. 1, par. 2).

Più nel dettaglio, il primo comma, nella versione attuale, sancisce che l'area precettiva delle disposizioni degli articoli 184, 185, 187-bis e 187-ter ricomprende:

a) gli strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, in un sistema multilaterale di negoziazione italiano o di altro Paese dell'Unione europea ovvero strumenti finanziari negoziati su un sistema organizzato di negoziazione (così mutuando la formulazione originaria della norma);

b) gli strumenti finanziari diversi da quelli dianzi esaminati, il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario menzionato nelle stesse lettere ovvero ha un effetto su tale prezzo o valore, compresi, a titolo esemplificativo, i credit default swap e i contratti differenziali;

c) le condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010.

Il successivo comma puntualizza che la manipolazione del mercato (artt. 185 e 187-ter T.U.F.) ben può avere ad oggetto: i) i contratti a pronti su merci diversi dai prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari enucleati dall'art. 180, comma primo, lett. a) T.U.F.; ii) gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci,

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari; iii) gli indici di riferimento (benchmark).

Mentre il comma terzo (di nuovo conio) positivizza che le norme incriminatrici degli abusi di mercato si applicano a qualsiasi operazione, ordine o altra condotta relativi agli strumenti finanziari di cui sopra, indipendentemente dal fatto che tale operazione, ordine o condotta avvenga in una sede di negoziazione.

L'intervento operato sull'art. 183 T.U.F. («Esenzioni») è, invece, volto ad escludere dall'ambito di applicazione dei market abuse le negoziazioni di azioni proprie effettuate ai sensi dell'art. 5 del Regolamento (UE) n. 596/2014, dando così concreta risposta alla censura mossa in tal senso dalla Commissione europea.

Di assoluto rilievo è la modifica apportata al delitto di insider trading di cui all'art. 184 T.U.F., la cui nuova rubrica risulta essere del seguente tenore: «Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate».

La prima modifica sostanziale introdotta si declina nell'inasprimento del trattamento sanzionatorio previsto per il c.d. insider primario, ovverosia il soggetto che sia a conoscenza di informazioni privilegiate «in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una o di una funzione, anche pubblica, o di un ufficio» (comma primo) e per il c.d. criminal insider che dispone delle notizie price sensitive informazioni privilegiate «a motivo della preparazione o dell'esecuzione di attività delittuose» (comma secondo). Infatti, per effetto della novella in disamina, l'attuale pena della reclusione da uno a sei anni è stata innalzata a due anni nel minimo e dodici anni nel massimo, unitamente alla previsione di una multa da ventimila a tre milioni di euro.

In verità, la novità più notevole e impattante è rappresentata dalla previsione dell'autonoma responsabilità penale dell'insider secondario, dovendosi intendere per tale il soggetto che compie una condotta di trading (acquisto, vendita o compimento di altre operazioni sugli strumenti finanziari), di tipping (comunicazione dell'informazione

privilegiata ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato) ovvero di tuyautage (raccomandare o indurre altri, sulla base dell'informazione privilegiata, al compimento di operazioni di trading), essendo venuto in possesso di informazioni privilegiate per ragioni diverse da quelle indicate ai precedenti commi e conoscendo il carattere privilegiato di tali informazioni, «fuori dai casi di concorso nei reati di cui ai commi 1 e 2».

Sino ad oggi l'insider secondario poteva essere destinatario della sanzione penale prevista dall'art. 184 T.U.F. soltanto nei casi di concorso con l'insider primario. Ma con l'entrata in vigore della modifica legislativa, l'insider secondario risponde oggi di un titolo autonomo di reato, seppur punito con una sanzione meno gravosa, id est la reclusione da un anno e sei mesi a dieci anni, unitamente alla multa da ventimila a due milioni e mezzo di euro. Inoltre, l'art. 184, comma 3, T.U.F. consente di aumentare la multa fino al triplo o fino al maggior importo di dieci volte il prodotto o il profitto conseguito dal reato quando questa appaia inadeguata per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito.

Si badi che, in ogni caso, resta salva l'applicabilità del più gravoso trattamento sanzionatorio regolato dall'art. 184, comma 1, T.U.F., laddove la condotta dell'insider secondario configuri un concorso nel reato dell'insider primario.

Altrettanto meritevole di nota è l'avvenuta interpolazione del comma quinto, a tenore del quale le previsioni dell'art. 184 T.U.F. si applicano anche alle condotte o alle operazioni relative «alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari».

Ancora, deve osservarsi che con l'abrogazione degli artt. 184, comma 3-bis e 185, commi 3-bis e 3-ter, T.U.F. è venuto meno il trattamento sanzionatorio più mite previsto per le fattispecie di abuso di informazione privilegiata e di manipolazione del mercato relative ad operazioni concernenti strumenti sui sistemi multilaterali di negoziazione e sui sistemi organizzati di negoziazioni ovvero quelle riguardanti altri strumenti quali, a mero titolo esemplificativo, i crediti swap o contratti differenziali.

Roma · Corso d'Italia, 29 - 00198
www.b-hse.law · info@b-hse.law · Tel. +39 06 99315900

Da ultimo, la Legge europea ha modificato l'art. 187 T.U.F. nel senso di limitare l'operatività della confisca, anche per equivalente, del solo profitto del reato di market abuse, con conseguente esclusione del prodotto e dei beni strumentali alla perpetrazione dell'illecito.

4. I riflessi delle modifiche legislative sulla responsabilità legislativa da reato *ex* D.Lgs. n. 231 del 2001

Le novità fin qui passate in rassegna comportano degli effetti non trascurabili anche sul piano della responsabilità amministrativa da reato, dal momento che la maggior parte delle norme incriminatrici modificate sono annoverate nel catalogo dei reati-presupposto di cui all'art. 24 e ss. del D.Lgs. n. 231 del 2001 (d'ora in avanti "il Decreto").

In particolar modo, i delitti informatici di cui agli artt. 615-quater, 615-quinquies, 617-quater e 617-quinquies c.p. costituiscono i predicate crimes dell'illecito amministrativo previsto dall'art. 24-bis del Decreto («Delitti informatici e trattamento illecito di dati»). I market abuse configurano invece, sin dal 2005, il presupposto oggettivo dell'illecito disciplinato dall'art. 25-sexies.

L'estensione del perimetro di applicazione delle norme incriminatrici in commento si traduce, con ogni evidenza, nella dilatazione dell'area del rischio astratto di commissione dei relativi reati-presupposto.

Il che impone alle società e agli enti che si sono già dotati di un Modello di Organizzazione, Gestione e Controllo un momento di serio approfondimento, al fine di valutare, sulla scorta della precedente attività di Risk Assessment, la rilevanza dei nuovi rischi in relazione alla propria operatività e di identificare con accuratezza le aree aziendali sensibili al mutato rischio di reato, oltre che di valutare l'adeguatezza dei presìdi di controllo già implementati, in una prospettiva di gap analysis.