OSSERVATORIO COMPLIANCE 231

di Morri Rossetti

Monthly Roundup

Novembre 2024

il verificarsi degli elementi tipici della truffa, quali gli artifizi e raggiri e l'induzione in errore.

La Corte non ha però aderito a tale interpretazione, giungendo a confermare il principio, già espresso in passato, secondo cui "*il riconoscimento del credito d'imposta previsto dalla legislazione in materia di bonus edilizi a seguito della trasmissione di false fatture attestanti l'esecuzione di opere in realtà mai effettuate integra una condotta riconducibile al parametro di cui all'art. 640 bis c.p. e non anche alla più lieve fattispecie dell'art. 316 ter c.p. posto che il riconoscimento del credito da parte dell'ente pubblico è avvenuto a seguito dell'induzione in errore dello stesso*".

A parere della Corte, infatti, la semplice emissione di false fatture basterebbe per configurare gli artifizi e i raggiri e non sarebbe necessaria un'attività di controllo preventivo circa la spettanza del credito da parte dell'Agenzia delle entrate per potersi dire integrata l'induzione in errore tipica del reato di truffa.

Per tale ragione, i fatti oggetto del procedimento sarebbero stati correttamente qualificati ai sensi dell'art. 640 bis c.p. anziché sussunti nella diversa fattispecie, meramente residuale, di indebita percezione di erogazioni pubbliche.

In aggiunta alle argomentazioni sin qui rappresentate, i giudici di legittimità hanno altresì approfondito il tema del momento consumativo del reato di truffa, affermando che "*essendosi in presenza di crediti per lavori inesistenti, ai fini del perfezionamento del reato e della sua consumazione, non occorre necessariamente individuare che l'ultimo cessionario porti in compensazione le somme con l'Agenzia delle entrate e ne ottenga la liquidazione, essendo sufficiente che anche la sola prima cessione abbia comportato il pagamento di somme non dovute al cessionario*".

Sotto questo profilo, la Cassazione si è discostata da un opposto orientamento secondo il quale, invece, il reato di truffa *ex* art. 640 bis può dirsi consumato solo quando il danno per lo Stato si sia concretamente configurato e, a sua volta, il danno può dirsi effettivamente realizzato solo quando i crediti fiscali ceduti siano stati materialmente riscossi o compensati (Cass. Pen., Sez. III, sent. n. 23402/2024).

Solo in tale eventualità, infatti, si verificherebbe la concreta perdita del denaro, siccome erogato a rimborso di un credito fittizio ovvero non incassato per effetto di compensazione con un credito fittizio.

Prima del verificarsi del danno così inteso in capo allo Stato, aggiunge la giurisprudenza che aderisce a questo secondo orientamento, può sussistere esclusivamente il tentativo di reato di truffa ai danni dello Stato o, eventualmente, la truffa in danno dei cessionari.

Merita, infine, evidenziare che anche in relazione all'altro tema trattato nella sentenza in commento – relativo all'integrazione del più grave reato di truffa ai danni dello Stato anziché di indebita percezione di erogazioni pubbliche – non vi è totale unanimità nelle pronunce dei giudici di merito e di legittimità.

Infatti, benché i principi affermati dalla Corte nella sentenza 40015/2024 rappresentino l'orientamento principale e maggiormente diffuso, non mancano pronunce di senso contrario che, al ricorrere di elementi fattuali analoghi a quelli oggetto del presente procedimento, hanno ritenuto di qualificare ai sensi dell'art. 316 ter c.p. le condotte di indebito ottenimento di bonus edilizi (Cass. Pen. Sez. II, n. 37138/2023).

* * *

Schema di Linee Guida in materia di *whistleblowing* sui canali interni di segnalazione: le indicazioni integrative fornite da ANAC nel suo recente documento

Lo scorso 7 novembre è stato pubblicato lo Schema di Linee guida in materia di *whistleblowing* sui canali interni di segnalazione adottato da ANAC a completamento e integrazione delle indicazioni già fornite con la delibera del 12 luglio 2023, n. 311.

L'obiettivo delle Linee Guida è garantire un'applicazione uniforme ed efficace della normativa sul *whistleblowing* e indirizzare ulteriormente i soggetti tenuti a dare attuazione alla stessa.

Nell'elaborazione del documento si è innanzitutto tenuto conto dei risultati del monitoraggio sullo stato di attuazione della normativa sul *whistleblowing*, condotta da ANAC nel 2023 attraverso sondaggi svolti in entrambi gli ambiti pubblico e privato.

L'analisi dei dati raccolti ha evidenziato "significative criticità", tra le quali la necessità di migliorare la comunicazione interna, la formazione del personale e la gestione dei canali di segnalazione.

Al fine di chiarire alcuni aspetti normativi e operativi, in questo schema di Linee Guida ANAC fornisce indicazioni chiare e indirizzi interpretativi di carattere generale, certamente utili ad orientare l'operato dei soggetti destinatari della normativa.

In particolare, si segnala innanzitutto la presenza di indicazioni di dettaglio sul **ruolo delle organizzazioni sindacali** al momento dell'attivazione di un nuovo canale di segnalazione interno.

Quanto ai suggerimenti forniti in relazione alle **modalità di effettuazione della segnalazione**, si sottolinea l'importanza della predisposizione di un canale di segnalazione in forma orale, alternativa a quella scritta, e della previsione di idonee modalità di tracciamento delle segnalazioni orali (ad esempio mediante registrazione ovvero verbalizzazione).

Di grande interesse appaiono altresì le indicazioni fornite in merito alle **necessità di adeguamento del Modello Organizzativo**, che – al fine di rispondere pienamente alla disciplina dettata dal D.lgs. 24/2023 – dovrebbe essere rivisto sotto almeno tre profili:

1. Previsione di un canale di segnalazione interna o adeguamento del canale precedentemente attivato per le violazioni del Modello;
2. Esplicitazione del divieto di ritorsione;
3. Aggiornamento del sistema disciplinare con possibili sanzioni nei confronti dei responsabili degli illeciti sanzionati da ANAC.

Rispetto al punto 1), le Linee Guida forniscono utili delucidazioni sul **coordinamento tra il "vecchio" sistema di segnalazione eventualmente in essere ai sensi dell'art. 6 co. 2 bis D.lgs. 231/01 e il nuovo sistema previsto dalla normativa che attua la Direttiva**.

Lasciando alle aziende la facoltà di decidere se mantenere entrambi i sistemi separati o se istituire un unico canale nel quale far confluire le

segnalazioni sia di violazioni del D.lgs. 231/01 del Modello Organizzativo che di violazioni previste dal D.lgs. 24/2023, l'Autorità si esprime in favore della seconda delle predette opzioni.

Il doppio canale, infatti, rischierebbe di essere una duplicazione e di porsi in contrasto con l'esigenza di semplificazione e razionalizzazione dei presidi esistenti. Inoltre, osserva l'ANAC, la presenza di due canali potrebbe ingenerare più confusione e rendere più gravosa, per la platea dei potenziali segnalanti, l'individuazione del corretto interlocutore a cui rivolgersi.

Qualora, invece, si optasse per la duplicità del canale, il segnalante si troverebbe dinnanzi all'alternativa di:

- Effettuare la segnalazione relativa alla violazione del Modello Organizzativo all'OdV, che la gestirebbe come un ordinario flusso informativo, con la conseguente esclusione dell'operatività delle tutele previste dal D.lgs. 24/2023 nei confronti del segnalante;
- Utilizzare il canale di segnalazione istituito in base alla normativa *Whistleblowing* così godendo di tutte le tutele previste dal decreto.

Dal suo lato l'OdV, nel ricevere la segnalazione, dovrebbe richiedere al segnalante se intenda beneficiare delle tutele garantite dalla legge in favore del *whistleblower* e, in caso di risposta affermativa, dovrebbe trasmettere la segnalazione al gestore delle segnalazioni *whistleblowing* (se soggetto diverso dall'OdV) e darne notizia al segnalante.

Nello Schema di Linee Guida si trovano anche alcuni suggerimenti per garantire il **coordinamento tra il gestore e l'OdV** (qualora non coincidano), nelle ipotesi in cui la segnalazione abbia ad oggetto una violazione del Modello Organizzativo.

Merita, infine, evidenziare le indicazioni fornite da ANAC in merito alle **modalità di gestione dei canali di segnalazione nell'ambito di gruppi societari**.

Partendo dalle posizioni prese sul tema dalla Commissione europea e bilanciandole con la normativa nazionale, ANAC ritiene che i gruppi di società possano valutare le seguenti soluzioni differenziate a seconda che si tratti di gruppo di medie o di grandi dimensioni:

- Gruppi di medie dimensioni (fino a 249 dipendenti): ammessa la condivisione di canale interno, attraverso l'istituzione di una piattaforma unica che, però, deve essere ramificata a livello di gruppo, consentendo al segnalane di scegliere da un elenco le società presso cui effettuare la segnalazione.
- Gruppi di grandi dimensioni (più di 249 dipendenti): la condivisione del canale interno e della gestione delle segnalazioni non è consentita. Eventualmente si potrebbe optare per l'esternalizzazione del servizio di ricezione e gestione della segnalazione a un fornitore esterno.

Infine, oltre a sottolineare l'importanza della formazione sia per i gestori che per i destinatari della procedura *Whistleblowing*, l'ANAC suggerisce di prevedere la presenza di sostituti dei gestori non solo nelle ipotesi di conflitto di interessi, ma anche nel caso di una loro assenza temporanea.

* * *

Decreto NIS 2: nuovi obblighi per le imprese in materia di *cybersecurity*

Il 1° ottobre è stato pubblicato in Gazzetta Ufficiale il D.lgs. n. 138/2024, che recepisce la Direttiva UE 2022/2555 (c.d. NIS 2) relativa a misure per un livello comune elevato di *cybersicurezza* dell'Unione.

Oltre a stabilire una strategia nazionale di cybersicurezza e a indicare i compiti delle diverse autorità pubbliche responsabili della tutela della sicurezza nazionale, il Decreto determina i criteri per l'individuazione dei soggetti cui si applicheranno precisi obblighi di sicurezza informatica.

Tra i settori toccati dalla normativa vi sono, tra gli altri, quello sanitario, energetico, telecomunicazioni e servizi digitali, bancario, finanziario e assicurativo.

Le imprese coinvolte dovranno prepararsi ad adottare misure volte a garantire resilienza delle infrastrutture, protezione dei dati e riduzione dei rischi.

Fondamentale a tal riguardo sarà la definizione di politiche di sicurezza informatica, nonché di piani di risposta agli incidenti e di *business continuity* e *disaster recovery*, svolgimento di *penetration test* e formazione in ambito *cybersecurity*.

Le misure di sicurezza peraltro dovranno essere rispettate anche dai fornitori, così imponendo alle imprese l'estensione di rigorosi controlli sulla *supply chain* anche in relazione ai rischi IT.

Il contributo è stato realizzato per la Newsletter Norme & Tributi del mese di ottobre 2024 di AHK Italien dal Dipartimento Diritto Penale dell'Economia e dell'Impresa di Morri Rossetti.

La Newsletter Norme & Tributi di AHK Italien relativa al mese di ottobre 2024 è disponibile qui.

Per maggiori informazioni e approfondimenti

Francesco Rubino
Partner e Responsabile Osservatorio Compliance 231

Francesco.Rubino@MorriRossetti.it

Morri Rossetti

Osservatorio 231

OSSERVATORIO
COMPLIANCE 231
di Morri Rossetti

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-231.it