

OSSERVATORIO
COMPLIANCE 231
di Morri Rossetti & Franzosi

Monthly Roundup

Ottobre 2026

Ottobre 2026

I principali aggiornamenti in materia di 231 dello scorso mese.

Dichiarazione fraudolenta: la consapevolezza della falsità non è sufficiente a provare il fine di evasione



Con la sentenza n. 31782 del 24 agosto 2026, la Terza Sezione penale della Corte di cassazione ha ribadito che, nel delitto di dichiarazione fraudolenta mediante uso di fatture per operazioni inesistenti, la consapevolezza della fittizietà dell'operazione non è di per sé sufficiente a provare il dolo specifico di evasione. Quest'ultimo richiede un autonomo accertamento e deve essere valutato anche alla luce delle condotte successive dell'imputato, comprese l'adesione all'accertamento tributario e l'esecuzione di pagamenti parziali.

1. L'inesistenza della fattura e la contestazione del fine evasivo

La vicenda ha avuto origine dalla contestazione del delitto di dichiarazione fraudolenta mediante uso di fatture per operazioni inesistenti, previsto dall'art. 2 del D.Lgs. n. 74/2000, formulata nei confronti di un contribuente per l'utilizzazione in dichiarazione di una fattura, dell'importo di euro 70.000 oltre IVA, relativa a **prestazioni** che i giudici di merito hanno ritenuto **oggettivamente inesistenti**.

Alla condanna pronunciata dal Tribunale è seguita la sostanziale conferma della Corte d'appello, che ha riconosciuto le attenuanti generiche e ridotto la pena a un anno di reclusione.

A fondamento dell'inesistenza dell'operazione, i giudici territoriali hanno valorizzato, tra l'altro, l'indeterminatezza della descrizione contenuta nella fattura, l'assenza di documentazione esterna idonea a comprovare l'effettività della prestazione, l'esistenza di due esemplari della medesima fattura con descrizioni differenti, la mancata tracciabilità del relativo pagamento e l'inconsistenza strutturale della società emittente.

L'imputato ha proposto ricorso per cassazione contestando sia l'accertamento dell'inesistenza oggettiva dell'operazione, sia la sussistenza dell'elemento soggettivo. Sotto quest'ultimo profilo, la difesa ha censurato l'automatismo attraverso il quale la Corte territoriale ha **desunto il dolo di evasione da circostanze inerenti alla materialità della condotta**, senza attribuire adeguato rilievo alle successive iniziative del contribuente, che aveva aderito all'accertamento tributario ed eseguito pagamenti parziali nell'ambito della definizione del debito fiscale.

2. Consapevolezza della falsità e fine di evasione: due accertamenti distinti

La Suprema Corte ha ritenuto inammissibili le censure relative all'elemento oggettivo, ritenendo adeguatamente motivato l'accertamento dell'inesistenza della prestazione. Ha invece **accolto il motivo relativo all'elemento soggettivo, annullando la sentenza con rinvio**.

Con riguardo all'art. 2 D.Lgs. n. 74/2000, la Cassazione ha ricordato che la fattispecie richiede, accanto alla consapevole utilizzazione in dichiarazione di elementi passivi fittizi, il **dolo specifico di evasione**, vale a dire la **finalità di evadere le imposte sui redditi o l'IVA, ovvero di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta**, la quale deve sussistere al momento della presentazione della dichiarazione e **non coincide con la mera consapevolezza della fittizietà dell'operazione**.

In questa prospettiva, secondo la Corte, l'annotazione della fattura in contabilità e la sua utilizzazione nella dichiarazione fiscale, in quanto elementi tipici della fattispecie, **non sono di per sé idonee a dimostrare il fine di evasione**. Diversamente opinando, si finirebbe infatti per sovrapporre la prova della consapevolezza dell'inesistenza della prestazione a quella della specifica finalità richiesta dalla norma incriminatrice.

Particolare rilievo assume, inoltre, la **valorizzazione delle condotte successive al fatto**. Se il mancato pagamento dell'imposta può concorrere, secondo la giurisprudenza di legittimità, a dimostrare il dolo specifico, il medesimo criterio inferenziale impone di considerare anche le circostanze di segno contrario. Nel caso esaminato, pertanto, l'adesione all'accertamento fiscale e i pagamenti parziali eseguiti dal contribuente avrebbero dovuto essere specificamente ponderati ai fini della ricostruzione dell'originaria finalità evasiva.

La pronuncia si colloca dunque nel solco dell'orientamento che configura il delitto di cui all'art. 2 D.Lgs. n. 74/2000 come fattispecie caratterizzata da dolo specifico, ma ne precisa le conseguenze sul terreno probatorio: **la prova dell'elemento oggettivo, anche quando particolarmente solida, non assorbe quella della finalità evasiva**. Non si tratta, pertanto, di un mutamento di indirizzo, quanto di una significativa puntualizzazione di principi già affermati dalla giurisprudenza di legittimità.

Sul piano pratico, l'arresto richiama l'attenzione sulla necessità di evitare automatismi nell'accertamento della responsabilità penal-tributaria. La **distinzione tra consapevolezza dell'inesistenza dell'operazione e finalità di evasione impone una valutazione complessiva del comportamento dell'imputato**, nella quale anche le **condotte successive di regolarizzazione** del rapporto tributario possono assumere rilievo probatorio.

Resta tuttavia necessario evitare l'automatismo opposto: adesione e pagamenti non escludono di per sé il dolo originario, ma costituiscono elementi che il giudice è tenuto a valutare nel complessivo quadro indiziario. È proprio in questa necessaria verifica individualizzata che la pronuncia mostra il suo maggiore interesse applicativo.

* * *

Whistleblowing: la riservatezza del segnalante non si ferma alla piattaforma



Un canale informatico sicuro non basta se le modalità degli accertamenti effettuati dal Gestore consentono di risalire all'autore della segnalazione. Con la delibera n. 344 del 9

settembre 2026, ANAC ha sanzionato i tre componenti dell'Organo di gestione delle segnalazioni di una società, richiamando la necessità di proteggere l'identità del whistleblower anche durante l'istruttoria.

Il caso e la decisione dell'Autorità

La vicenda riguarda una segnalazione, trasmessa attraverso la piattaforma aziendale, relativa a presunte irregolarità contrattuali. Per verificarne il contenuto, l'Organo di gestione aveva intervistato i componenti del ristretto gruppo di lavoro coinvolto, fornendo indicazioni sull'esistenza della segnalazione, sul contratto interessato e sulla documentazione allegata.

Secondo ANAC, queste informazioni, combinate con gli elementi di contesto già conosciuti dagli intervistati, permettevano di individuare il segnalante. Le modalità dell'indagine avevano così vanificato la protezione originariamente assicurata dalla piattaforma crittografata. L'Autorità ha quindi irrogato **una sanzione di 15.000 euro a ciascuno dei tre componenti** per violazione dell'obbligo di riservatezza previsto dall'art. 12 del D.Lgs. 24/2023.

Le informazioni riservate

Il punto centrale del provvedimento è che la riservatezza non riguarda soltanto il nominativo del whistleblower. La tutela si estende a **qualsiasi informazione dalla quale la sua identità possa essere ricavata, anche indirettamente**.

In assenza del consenso espresso del segnalante, tali elementi non possono essere rivelati a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni ed espressamente autorizzate a trattare i relativi dati.

L'Autorità da rilievo all'idoneità delle informazioni comunicate a consentire l'individuazione del segnalante. Neppure il richiamo agli intervistati a mantenere riservato quanto appreso è sufficiente, perché non impedisce loro di dedurre autonomamente chi abbia presentato la segnalazione.

Spunti di riflessione e indicazioni operative

La delibera pone l'attenzione sulla necessità di **affiancare alle garanzie tecnologiche della piattaforma cautele concrete nella conduzione dell'istruttoria**. L'accertamento dei fatti deve essere organizzato tenendo conto della composizione del gruppo di lavoro, delle conoscenze degli interlocutori e del rischio che singoli dettagli, collegati tra loro, rendano riconoscibile il segnalante.

Per i gestori, ciò significa valutare preventivamente quali informazioni condividere e come impostare le interviste, adottando modalità di indagine capaci di preservare la riservatezza. La sicurezza del canale di ricezione è quindi un presidio necessario, ma deve trovare continuità nelle scelte di chi gestisce la segnalazione.

* * *

Dal rischio ignorato all'infortunio: le responsabilità di chi organizza il cantiere



Un albero da rimuovere, piani di sicurezza che non ne considerano la presenza e un'iniziativa del lavoratore imprudente. Con la sentenza n. 17541

del 2026, la Quarta Sezione penale della Cassazione conferma le responsabilità del datore di lavoro, del coordinatore per l'esecuzione e del committente statuendo che i vuoti organizzativi non possono essere colmati da un generico divieto, né ricondotti alla sola condotta imprudente del lavoratore.

Il caso e l'iter processuale

La vicenda trae origine dall'abbattimento di un albero che si trovava in prossimità di uno scavo. Per proseguire i lavori e completare l'opera occorreva rimuoverlo, ma nessuno dei documenti di sicurezza ne disciplinava l'abbattimento.
È attorno a questa omissione che ruota la vicenda esaminata dalla Cassazione. Un lavoratore dipendente di un'impresa artigiana perdeva la vita per le gravissime lesioni provocate dalla caduta dell'albero presente nel cantiere situato nel giardino di un'abitazione.

Il Tribunale di Genova affermava la responsabilità per omicidio colposo del titolare dell'impresa affidataria, del coordinatore per l'esecuzione e del committente, che aveva assunto anche la qualifica di responsabile dei lavori. La Corte d'appello confermava la condanna. I tre imputati ricorrevano quindi per cassazione, contestando, con argomentazioni diverse, il collegamento causale tra le rispettive omissioni e l'incidente.

Al centro delle difese degli imputati vi era l'iniziativa autonoma del lavoratore atteso che l'abbattimento sarebbe stato estraneo alle mansioni affidategli e contrario alle direttive ricevute. La Cassazione ha tuttavia rigettato i ricorsi e confermato la condanna dei ricorrenti.

L'imprudenza del lavoratore non esclude la responsabilità nei casi di vuoto organizzativo

Il punto decisivo non è stabilire soltanto se il lavoratore abbia agito di propria iniziativa. Occorre verificare se la sua condotta abbia attivato un rischio davvero estraneo alla sfera che i garanti erano tenuti a governare. La Corte ribadisce che, per interrompere il nesso causale, il comportamento del lavoratore deve essere **eccentrico o esorbitante rispetto al rischio affidato alla gestione del titolare della posizione di garanzia**.

Nel caso concreto, secondo i giudici di merito e la Corte di Cassazione la rimozione dell'albero non rappresentava un'attività scollegata dal cantiere. La conformazione dei luoghi e l'avanzamento delle opere la rendevano necessaria per proseguire lo scavo. Eppure, il piano operativo di sicurezza (POS) non conteneva indicazioni al riguardo e non era stata disposta la sospensione delle attività in attesa dell'intervento di un'impresa dotata delle competenze necessarie.

È questo vuoto a dare rilievo causale alle omissioni organizzative. Il lavoratore era stato lasciato senza una regolamentazione adeguata delle attività da svolgere e delle relative modalità esecutive. In tale contesto, secondo la Corte, **l'iniziativa imprudente non poteva essere qualificata come abnorme e utilizzata per escludere la responsabilità dei soggetti garanti**.

I piani di sicurezza devono considerare i rischi concreti

La pronuncia in esame tratta il tema della differenza tra un piano formalmente esistente e un piano realmente aderente al lavoro da eseguire. Il POS non disciplinava il punto di inizio e le fasi dello scavo, né menzionava il grosso albero presente nelle immediate vicinanze dello scavo. Il piano di sicurezza e coordinamento (PSC), a sua volta, seguiva un format prestabilito che non considerava l'effettiva morfologia dei luoghi.

Il documento, inoltre, non era stato adeguato all'evoluzione dei lavori e non risultava

coordinato con il POS. La responsabilità del coordinatore per l'esecuzione viene quindi ricondotta a omissioni precise: non avere considerato le peculiarità del cantiere, non avere verificato l'idoneità e la coerenza del piano dell'impresa e non avere assicurato l'adeguamento della pianificazione all'avanzamento delle opere.

La Cassazione sottolinea la necessità di individuare, analizzare e valutare **i rischi concreti relativi all'area, all'organizzazione del cantiere e alle lavorazioni**.

La responsabilità del committente

Un ulteriore profilo che merita di essere approfondito è quello che attiene al committente. La Corte conferma che la verifica dell'idoneità dell'impresa non può esaurirsi nella sua regolarità formale e contributiva ma deve riguardare anche aspetti concreti quali la disponibilità di maestranze qualificate e di mezzi adeguati alle concrete lavorazioni.
La nomina del coordinatore, inoltre, non esauriva gli obblighi del soggetto che aveva assunto anche il ruolo di responsabile dei lavori.

Spunti di riflessione e indicazioni operative

La sentenza in esame pone l'attenzione sul fatto che **i documenti di sicurezza devono descrivere il cantiere reale, non un cantiere astratto**. Ostacoli presenti nell'area, sequenze di scavo, cambiamenti delle lavorazioni e necessità di competenze specialistiche devono trovare una risposta nella pianificazione e nel suo aggiornamento, ciascuno nell'ambito delle rispettive attribuzioni.

Per le imprese e i professionisti coinvolti, ciò significa verificare la coerenza tra PSC e POS, disciplinare le fasi critiche e, quando manchino condizioni o competenze necessarie, non lasciare alla libera iniziativa dei lavoratori la risoluzione di problematiche che potrebbero insorgere. Per il committente, significa scegliere l'impresa in rapporto alle effettive esigenze dell'opera e non considerare la nomina del coordinatore come un esonero generalizzato dai propri doveri.

* * *

Intelligenza Artificiale: profili di impatto sistemico e ricadute sulla responsabilità 231



1. Il quadro di riferimento

Con il **decreto legislativo 9 settembre 2026, n. 160**, il legislatore ha dato attuazione al **Regolamento (UE) 2024/1689** (*AI Act*) con riferimento all'utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia e alla disciplina della responsabilità civile e penale connessa all'impiego di tali sistemi. Il provvedimento si inserisce nel solco tracciato dalla legge 23 settembre 2025, n. 132, recante deleghe al Governo in materia di intelligenza artificiale – e, in particolare, dall'articolo 24 di tale legge – e costituisce uno dei primi tasselli di adeguamento all'AI Act.

Il decreto si articola in tre direttrici principali: *(i)* la disciplina dell'**uso dell'IA nelle attività di polizia**, incluse ricerca, sperimentazione e sorveglianza biometrica; *(ii)* l'introduzione di **nuove fattispecie penali** e la corrispondente **estensione della responsabilità amministrativa degli enti ex d.lgs. 231/2001**; *(iii)* un nuovo istituto processuale civilistico per il **risarcimento**

dei danni cagionati dall'utilizzo di sistemi di IA.

Per quanto di interesse in questa sede, l'analisi avrà ad oggetto unicamente l'introduzione delle nuove fattispecie di reato e il conseguente ampliamento del catalogo dei reati presupposto della responsabilità amministrativa degli enti ex d.lgs. 231/2001.

2. Il nuovo art. 437-bis c.p.

Il Titolo II del D.lgs. 160/2026 innesta nel codice penale una fattispecie di rilievo sistematico, rubricata "***Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi***". Il nuovo **art. 437-bis c.p.** prevede e punisce condotte illecite eterogenee, riferibili a soggetti differenti lungo l'intera filiera dell'IA.

Il **primo comma** punisce con la reclusione da uno a cinque anni chiunque **ometta di adottare le misure tecniche di sicurezza** previste per la **progettazione**, **l'addestramento**, la **produzione** o **l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio**, idonee a prevenire **malfunzionamenti** o **alterazioni** del funzionamento dei sistemi, ovvero **ometta di adottare misure di sorveglianza umana**, laddove da tali omissioni derivi un **pericolo** per la vita o per l'incolumità pubblica o privata. Ove dalle medesime condotte derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni. Tali condotte omissive sono punite anche a titolo di **colpa grave**.

Il **secondo comma** punisce, salvo che il fatto costituisca più grave reato e al di fuori delle condotte sanzionate dal primo comma, chiunque **alteri sistemi di intelligenza artificiale ad alto rischio, con la pena della reclusione da due a sei anni, laddove** da tali condotte derivi un **pericolo** per la vita o per l'incolumità pubblica o privata. Ove dalle medesime condotte derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni.

Il **quarto** ed ultimo **comma** punisce infine con le pene previste dal primo comma **l'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio** che **ometta intenzionalmente di adottare misure di sorveglianza umana**, laddove da tale omissione derivi un **pericolo** per la vita o per l'incolumità pubblica o individuale, ovvero un pericolo per la sicurezza dello Stato.

Ne discende una chiara ripartizione soggettiva: l'omessa adozione di misure tecniche di sicurezza idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi è condotta rimproverabile a progettatori, addestratori, produttori e soggetti che immettono nel mercato sistemi di intelligenza artificiale ad alto rischio; l'alterazione di tali sistemi e l'omessa adozione di misure di sorveglianza umana sono invece condotte rimproverabili agli utilizzatori dei medesimi.

2.1. I sistemi di intelligenza artificiale ad alto rischio

Le nuove condotte penalmente rilevanti pocanzi illustrate sono connesse alla progettazione, addestramento, produzione, immissione sul mercato e utilizzo di **sistemi di intelligenza artificiale ad alto rischio.**

Il D.lgs. 160/2026 non fornisce una definizione autonoma di sistema di intelligenza artificiale ad alto rischio, rinviando integralmente al Regolamento (UE) 2024/1689 (*AI Act*).

Nello specifico, l'**art. 6 dell'AI Act** individua i sistemi di intelligenza artificiale ad alto rischio secondo due direttrici parallele: (*i)* sistemi di IA che costituiscono componenti di sicurezza di prodotti – o che sono essi stessi prodotti – coperti dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I al Regolamento e soggetti

a valutazione di conformità di terzi; *(ii)* sistemi di IA che ricadono in uno dei casi d'uso elencati nell'Allegato III al Regolamento (tra cui, a titolo esemplificativo, gestione delle infrastrutture critiche, istruzione, occupazione, accesso a servizi essenziali, attività di law enforcement e amministrazione della giustizia).

3. L'art. 612-quater c.p.

Accanto all'art. 437-bis c.p. si colloca l'art. 612-quater c.p., rubricato "***Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale***", introdotto dall'art. 26, comma 1, lett. c), della legge 23 settembre 2025, n. 132, e oggi assurto a reato presupposto della responsabilità degli enti.

Tale fattispecie rappresenta la prima incriminazione di parte speciale specificamente dedicata al fenomeno dei c.d. *deepfake*, volta a proteggere l'identità personale, la reputazione e l'autodeterminazione dell'individuo rispetto a rappresentazioni digitali falsificate o alterate della sua immagine, voce o sembianze, in linea di continuità con la tutela già offerta contro il c.d. *revenge porn*.

Il reato punisce chiunque cagioni un **danno ingiusto** ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati **mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità**.

4. L'ampliamento della responsabilità amministrativa degli enti

Il fulcro di maggiore impatto per gli operatori economici è rappresentato dall'art. 15 del D.lgs. 160/2026, che inserisce nel D.lgs. 231/2001, dopo l'articolo 25-*undevicies*, il **nuovo art. 25-*vicies*** ("Reati commessi con l'uso di sistemi di intelligenza artificiale"), il quale prevede:

i. la **sanzione pecuniaria** da seicento a mille quote in relazione al delitto di cui all'**art. 437-bis c.p.**
ii. la **sanzione pecuniaria** da duecento a settecento quote in relazione all'**art. 612-quater c.p.**
iii. in entrambi i casi l'applicazione delle **sanzioni interdittive** di cui all'articolo 9, comma 2, lettere b), c), d) ed e), del decreto.

Le implicazioni sistematiche sono molteplici.
In primo luogo, il catalogo dei reati presupposto si arricchisce di una fattispecie a struttura eminentemente **organizzativa e omissiva**: l'art. 437-bis c.p. sanziona l'omessa adozione di misure tecniche di sicurezza e di sorveglianza umana.

La responsabilità dell'ente si radica dunque non tanto in una condotta attiva del soggetto apicale o del sottoposto, quanto in una **carenza strutturale del sistema di controllo interno** sugli strumenti di intelligenza artificiale, con evidenti ricadute sui contenuti minimi del Modello di organizzazione, gestione e controllo.

In secondo luogo, la sostanziale coincidenza tra gli obblighi organizzativi imposti dall'*AI Act* e il perimetro dei nuovi reati presupposto genera un fenomeno di **compliance integrata**: l'adempimento sostanziale degli obblighi previsti dall'AI Act tende a coincidere con l'idoneità del Modello 231, con la possibilità di invocarne l'efficacia esimente anche in assenza di una compliance formalmente distinta, purché sostanzialmente coincidente e adeguatamente documentata.

Alla luce del quadro delineato, gli enti che sviluppano, immettono sul mercato o utilizzano sistemi di IA – e, in particolare, sistemi ad alto rischio – sono chiamati ad avviare un percorso di adeguamento del proprio sistema di *compliance* 231 finalizzato a:

i. **mappare** i tool di intelligenza artificiale;
ii. individuare e attribuire le **responsabilità** alle varie funzioni aziendali;
iii. individuare le necessarie **misure tecniche e/o di sorveglianza umana**;
iv. garantire una **tracciabilità** dei processi decisionali;
v. **aggiornare la mappatura dei rischi 231** e la matrice reati/processi includendo l'intero ciclo di vita dei sistemi di IA (progettazione, addestramento, produzione, immissione sul mercato, utilizzo e monitoraggio *post-market*);
vi. formalizzare **specifici protocolli** in tema di *data governance*, gestione dei *log*, valutazione dei rischi ex art. 9 AI Act e sorveglianza umana ex art. 14 AI Act;
vii. prevedere **flussi informativi** strutturati verso l'Organismo di Vigilanza in ordine agli incidenti, ai malfunzionamenti e alle segnalazioni ricevute in relazione ai sistemi di IA impiegati;
viii. integrare la **parte speciale** del Modello 231 con presidi dedicati anche al reato di cui all'art. 612-quater c.p., soprattutto ove l'ente svolga attività di produzione, editing o diffusione di contenuti multimediali.

5. Considerazioni conclusive

Il D.lgs. 160/2026 segna un punto di svolta nel rapporto tra intelligenza artificiale e responsabilità degli enti. L'inserimento nel catalogo dei reati presupposto di fattispecie a struttura marcatamente organizzativa – come l'art. 437-bis c.p. – e la contestuale previsione di **sanzioni pecuniarie particolarmente elevate** (fino a mille quote per il reato di cui all'art. 437-bis c.p.) accompagnate dall'applicazione di **sanzioni interdittive** ex art. 9, comma 2, lett. b), c), d) ed e), del decreto rendono l'adeguamento del Modello 231 una priorità non più differibile per tutti gli operatori che, a vario titolo, intervengono nella filiera dell'IA.

In prospettiva, il vero banco di prova sarà rappresentato dalla capacità delle imprese di costruire un sistema di *governance* dell'IA realmente integrato con il Modello 231, in cui i presidi tecnici richiesti dall'AI Act non si esauriscano in adempimenti formali ma si traducano in scelte organizzative documentate, tracciabili e verificabili.

Solo un approccio di questo tipo potrà consentire all'ente di beneficiare, in sede di eventuale procedimento, dell'efficacia esimente del Modello, evitando che l'omissione – tanto tecnica quanto di sorveglianza – si traduca in una responsabilità di natura sostanzialmente strutturale.

Per maggiori informazioni e approfondimenti

Francesco Rubino
Partner e Responsabile Osservatorio Compliance 231

Francesco.Rubino@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio 231**

OSSERVATORIO
COMPLIANCE 231
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-231.it