

# FOCUS

*IA E MODELLO 231:  
COME AFFRONTARE I NUOVI  
RISCHI PER L'IMPRESA?*

## 1. PREMESSA

Con il **D.Lgs. 9 settembre 2026, n. 160**, pubblicato in Gazzetta Ufficiale il 15 settembre 2026 ed entrato in vigore il successivo **30 settembre**, il legislatore delegato ha dato attuazione alla delega contenuta nell'art. 24 della legge 23 settembre 2025, n. 132 (la cosiddetta "*legge sull'IA*"), proseguendo nell'adeguamento dell'ordinamento interno al Regolamento (UE) 2024/1689 (cosiddetto "*AI Act*") sul versante della responsabilità civile e penale.<sup>1</sup>

Per quello che qui interessa, la novità di maggiore impatto per le imprese è l'introduzione nel D.Lgs. 231/2001 (di seguito, anche, il "*Decreto 231*") del **nuovo art. 25-vicies**, rubricato "*Reati commessi con l'uso di sistemi di intelligenza artificiale*", che inserisce nel catalogo dei reati presupposto due fattispecie: il nuovo delitto di **omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi** (art. 437-bis c.p.) e il delitto di **illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale** (art. 612-quater c.p.), introdotto dalla stessa legge n. 132/2025.

Giova sgombrare il campo, sin da subito, da un equivoco. La riforma **non introduce una responsabilità**

<sup>1</sup>() Il D.Lgs. n. 160/2026 reca "*Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 [...] in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale*".

**generalizzata dell'ente per qualsiasi violazione dell'AI Act**: la mera inosservanza degli obblighi regolatori resta presidiata dall'apparato sanzionatorio amministrativo europeo e nazionale. L'ente risponderà, invece, soltanto quando sia commesso uno dei due reati presupposto, nel suo interesse o a suo vantaggio, e ricorrano gli ordinari criteri di imputazione del Decreto 231.

Ciononostante, le ricadute potrebbero rivelarsi tutt'altro che marginali. Gli obblighi di sicurezza, di sorveglianza umana e di tracciabilità previsti dall'AI Act rischiano di non essere più un mero adempimento di *compliance* regolatoria e potrebbero diventare il parametro attraverso cui valutare l'**adeguatezza dell'organizzazione aziendale**: in altri termini, la tradizionale colpa di organizzazione potrebbe ora estendersi a anche il modo in cui l'impresa **seleziona, configura, sorveglia e documenta** l'impiego dei sistemi di IA.

Questo *focus*, dopo una breve analisi delle nuove fattispecie e dell'apparato sanzionatorio, si propone di individuare – senza pretesa di esaustività, in un quadro ancora in larga parte da esplorare – i principali **profili di rischio penale** cui sono oggi esposte le imprese che sviluppano o impiegano sistemi di intelligenza artificiale e di suggerire alcuni dei **presidi di controllo** più opportuni per prevenirli.

## 2. IL NUOVO ART. 25-VICIES DEL DECRETO 231

### 2.1 L'OMESSA ADOZIONE DI MISURE DI SICUREZZA E L'ALTERAZIONE DEI SISTEMI DI IA AD ALTO RISCHIO (ART. 437-BIS C.P.)

La nuova fattispecie, collocata immediatamente dopo l'art. 437 c.p. (rimozione od omissione dolosa di cautele contro infortuni sul lavoro), all'interno dei delitti contro l'incolumità pubblica, presenta una **struttura articolata**:

- il **primo comma** punisce con la reclusione da uno a cinque anni *"chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana"*, quando da tali omissioni derivi **pericolo per la vita o l'incolumità pubblica o individuale**; la pena è della reclusione da due a otto anni se ne deriva un pericolo per la **sicurezza dello Stato**;
- il **secondo comma**, con clausola di riserva, sanziona chiunque **altera** sistemi di intelligenza artificiale ad alto rischio, con la reclusione da due a sei anni (da tre a dieci anni nel caso di

pericolo per la sicurezza dello Stato);

- il **terzo comma** punisce i fatti di cui al primo comma anche se commessi per **colpa grave**, con pena ridotta;
- il **quarto comma**, infine, estende le pene del primo comma all'**utilizzatore professionale** (il *deployer*, nella terminologia dell'AI Act) che ometta **intenzionalmente** di adottare misure di sorveglianza umana.

Tre profili meritano di essere evidenziati.

*In primo luogo*, si tratta di un **reato di pericolo concreto**: non ogni malfunzionamento o *output* errato assume rilevanza penale, essendo necessario che dall'omissione derivi un pericolo effettivo per i beni giuridici tutelati.

*In secondo luogo*, l'ambito oggettivo è circoscritto ai soli sistemi qualificati **"ad alto rischio"** ai sensi dell'art. 6 e dell'Allegato III del Regolamento europeo (si pensi, a titolo esemplificativo, ai sistemi impiegati come componenti di sicurezza di prodotti, nella selezione del personale, nella valutazione del merito creditizio o nella gestione di infrastrutture critiche).

*In terzo luogo*, la fattispecie omissiva è a **forte eterointegrazione**: le *"misure tecniche di sicurezza previste"* e le misure di sorveglianza umana rinviano, inevitabilmente, agli obblighi di cui agli artt. 8-15 dell'AI Act (sistema di gestione dei rischi, governance dei dati, documentazione tecnica, registrazione

degli eventi, trasparenza, sorveglianza umana, accuratezza, robustezza e cybersicurezza), come integrati dalle norme tecniche armonizzate. Ne derivano prevedibili tensioni con i principi di riserva di legge e di determinatezza, ma anche – e soprattutto, nella prospettiva dell'impresa – la sostanziale **coincidenza tra la regola cautelare penalmente rilevante e l'obbligo regolatorio**.

## 2.2 L'ILLECITA DIFFUSIONE DI CONTENUTI GENERATI O ALTERATI CON SISTEMI DI IA (ART. 612-QUATER C.P.)

La seconda fattispecie richiamata dall'art. 25-*vicies* punisce con la reclusione da uno a cinque anni chi cagiona un **danno ingiusto** a una persona cedendo, pubblicando o altrimenti diffondendo, **senza il suo consenso**, immagini, video o voci falsificati o alterati mediante sistemi di IA e **idonei a indurre in inganno** sulla loro genuinità (i cosiddetti *deepfake*).

Non è dunque punita la mera creazione del contenuto sintetico, bensì la sua diffusione non consentita e lesiva. Per l'impresa, il punto di attenzione si sposta allora sui processi di **comunicazione, marketing, gestione del personale** e, più in generale, su tutti i canali attraverso i quali l'ente pubblica contenuti per conto proprio. Va peraltro segnalato che gli obblighi di *disclosure* previsti dall'*AI Act* per i contenuti sintetici non sostituiscono il consenso dell'interessato né escludono, di per sé, il danno.

## 2.3 IL TRATTAMENTO SANZIONATORIO DELL'ENTE

Sul piano delle conseguenze per l'ente, l'art. 25-*vicies* prevede:

- per il delitto di cui all'art. 437-*bis* c.p., la **sanzione pecuniaria da seicento a mille quote**: una cornice che colloca la fattispecie nella fascia più elevata del catalogo e che, considerato il valore massimo della singola quota (euro 1.549), comporta un'esposizione teorica fino a circa **1,5 milioni di euro**;
- per il delitto di cui all'art. 612-*quater* c.p., la **sanzione pecuniaria da duecento a settecento quote**;
- per entrambe le fattispecie, le **sanzioni interdittive** di cui all'art. 9, comma 2, lett. b), c), d) ed e), del Decreto 231: la sospensione o revoca di autorizzazioni, licenze o concessioni; il divieto di contrattare con la Pubblica Amministrazione; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

## 3. I RISCHI PENALI PER L'IMPRESA

### 3.1 INTERESSE O VANTAGGIO: IL RISPARMIO SUI COSTI DELLA SICUREZZA TECNOLOGICA

Il primo banco di prova è il criterio oggettivo di imputazione di cui all'art. 5 del Decreto 231.

Rispetto alle forme dolose (si pensi all'alterazione di un sistema per comprimere i costi di adeguamento o per conseguire *performance* commercialmente spendibili) l'accertamento non presenta particolari peculiarità. È sulla forma **colposa** che si concentra il rischio maggiore.

Come noto, a partire dalla sentenza delle Sezioni Unite sul caso *ThyssenKrupp* (Cass. Pen., SS.UU., 18 settembre 2014, n. 38343), la giurisprudenza riferisce l'interesse o il vantaggio dell'ente non all'evento, bensì alla **condotta violativa della regola cautelare**: integra il criterio di imputazione il risparmio di costi, la velocizzazione dei processi o la massimizzazione della produzione conseguiti attraverso la violazione delle cautele.

Lo schema potrebbe trovare nell'economia dell'IA un terreno particolarmente fertile, sebbene manchino, allo stato, precedenti applicativi. La compressione del *time-to-market*, la riduzione degli investimenti in *testing* e validazione, il contenimento dei costi della sorveglianza umana – che, per definizione, richiede risorse dedicate ed è quindi il primo candidato al taglio in ottica di efficienza – o lo svolgimento meramente cartolare della valutazione di conformità sono condotte che potrebbero essere agevolmente ricondotte a un **interesse economico apprezzabile dell'ente**. Secondo l'orientamento formatosi in materia di sicurezza sul lavoro (art. 25-*septies*),

peraltro, anche un risparmio modesto, purché non irrisorio, è idoneo a integrare il criterio; resta tuttavia da verificare se – e con quali adattamenti – tale orientamento sarà esteso alla nuova fattispecie.

### 3.2 LA COLPA DI ORGANIZZAZIONE "ALGORITMICA"

Sul versante soggettivo operano i consueti criteri degli artt. 6 e 7 del Decreto 231. Nelle organizzazioni che sviluppano o impiegano IA ad alto rischio, tuttavia, le decisioni rilevanti ai fini della fattispecie omissiva – l'allocazione dei *budget* di sicurezza, l'approvazione del rilascio di un sistema, la definizione del perimetro della sorveglianza umana, l'accettazione di rischi residui – sono tipicamente **decisioni apicali**: è dunque plausibile – ma non scontato – che il contenzioso si concentri sull'ipotesi di cui all'art. 6, con la connessa **inversione dell'onere probatorio** a carico dell'ente.

La colpa di organizzazione potrebbe assumere, in questo contesto, una fisionomia peculiare, che parte della dottrina ha già definito "*algoritmica*": il rimprovero all'ente non riguarda soltanto l'omessa adozione di procedure, ma l'**inadeguato governo di un agente tecnologico semi-autonomo**, i cui *output* non sono integralmente prevedibili. Il giudizio di idoneità del Modello sarà, verosimilmente, chiamato a misurarsi con interrogativi inediti: il malfunzionamento era prevedibile? Il sistema di gestione dei rischi copriva

quello scenario? La sorveglianza umana era **effettiva** o meramente formale (il cosiddetto *rubber-stamping* dell'operatore che convalida acriticamente l'*output* della macchina)?

### 3.3 L'AUTORE NON IDENTIFICATO (ART. 8 DEL DECRETO 231)

Un profilo che potrebbe acquisire rilevanza pratica inedita è quello dell'art. 8 del Decreto 231, ai sensi del quale la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato.

Nella filiera dell'IA, la **parcellizzazione dei contributi** (progettazione, addestramento, configurazione, manutenzione, impiego) può rendere genuinamente impossibile attribuire la violazione cautelare a una persona fisica determinata, pur essendo evidente la sua matrice organizzativa. Il rischio è che la colpa grave individuale venga desunta dalla macroscopica inadeguatezza dell'assetto organizzativo, con una deriva verso forme di responsabilità diretta dell'ente che il sistema, allo stato, non autorizza. È prevedibile che su questo terreno si registrino oscillazioni interpretative, la cui composizione sarà inevitabilmente affidata alla giurisprudenza.

### 3.4 IL RISCHIO CAUTELARE: INTERDITTIVE E SEQUESTRI

Come anticipato, le sanzioni interdittive richiamate dall'art. 25-*vicies* possono essere applicate in via cautelare ai sensi degli artt. 45 ss. del Decreto 231, in presenza di gravi indizi di responsabilità e di concreto pericolo di

reiterazione, con effetti potenzialmente paralizzanti ben prima di qualunque accertamento di merito.

Sul versante reale, il sequestro preventivo potrà investire sistemi, piattaforme, *server*, modelli addestrati e *dataset*, aggredendo il **patrimonio tecnologico** dell'impresa con danni difficilmente reversibili. Quanto alla confisca del profitto (art. 19), trattandosi di un reato di pericolo, il profitto confiscabile potrebbe essere individuato – ma la questione è tutt'altro che pacifica – nel **risparmio di spesa** derivante dalle misure di sicurezza omesse, secondo lo schema già sperimentato in materia ambientale e antinfortunistica.

Non va trascurato, inoltre, che l'emersione del reato non passerà necessariamente da un incidente: potrà originare da segnalazioni delle autorità di vigilanza (*in primis*, l'Agenzia per la Cybersicurezza Nazionale), da *incident report*, da *audit* ispettivi o da segnalazioni *whistleblowing*, con un possibile ampliamento delle occasioni di contestazione.

### 3.5 UN RISCHIO TRASVERSALE: LE INTERFERENZE CON IL CATALOGO ESISTENTE

Il rischio da intelligenza artificiale non resta confinato al perimetro dell'art. 25-*vicies*. Esso permea l'intero catalogo dei reati presupposto, per almeno tre ragioni:

- l'**aggravante comune** di cui all'art. 61, n. 11-*decies*, c.p., introdotta dalla legge n.

132/2025 (reato commesso mediante sistemi di IA che abbiano costituito mezzo insidioso, ostacolato la difesa o aggravato le conseguenze del reato), è applicabile a **tutti i reati presupposto**;

- talune fattispecie già presenti nel catalogo sono state arricchite di **aggravanti speciali** legate all'impiego di IA: è il caso dell'aggitaggio (art. 2637 c.c., richiamato dall'art. 25-ter) e della manipolazione del mercato (art. 185 TUF, richiamato dall'art. 25-sexies);
- l'impiego di IA ad alto rischio in contesti produttivi (robotica collaborativa, manutenzione predittiva, controllo degli accessi) costituisce il punto di sutura con i reati in materia di **salute e sicurezza sul lavoro** (art. 25-septies), mentre l'alterazione di un sistema potrà frequentemente integrare, a monte, condotte di accesso abusivo o danneggiamento informatico (art. 24-bis).

Ne discende che, in caso di evento lesivo, la contestazione all'ente potrà cumulare più illeciti, con conseguente **moltiplicazione dell'esposizione sanzionatoria**.

#### 4. I PRESIDI DI CONTROLLO PIÙ OPPORTUNI

La riforma non impone una *checklist* né un registro dei sistemi di IA. Mette, però, alla prova il **Modello di organizzazione, gestione e controllo**.

Non sarà quindi sufficiente una modifica meramente compilatoria: l'aggiornamento dovrebbe essere sostanziale e auspicabilmente tempestivo, pur nella consapevolezza che, in assenza di prassi applicative consolidate, i presidi di seguito indicati non possono che essere individuati in via prudenziale e non offrono, di per sé, alcuna garanzia di esonero dalla responsabilità.

#### 4.1 LA MAPPATURA DEI SISTEMI E DEI RUOLI

Un primo passaggio potrebbe consistere nell'aggiornamento del **risk assessment**, che dovrebbe:

- censire i sistemi di IA in uso o in sviluppo (cosiddetto *AI inventory*), **inclusa la cosiddetta shadow AI**, ossia l'impiego non censito di strumenti di IA da parte delle funzioni aziendali, che sottrae il rischio alla mappatura e costituisce, di per sé, un *deficit* organizzativo;
- qualificare ciascun sistema secondo la tassonomia dell'AI Act, con particolare attenzione alla classificazione "*ad alto rischio*";
- identificare il **ruolo** rivestito dall'ente nella filiera (*provider*, *deployer*, importatore, distributore), da cui dipende il perimetro degli obblighi cautelari la cui violazione integra la condotta tipica;
- collegare i sistemi ai **processi sensibili** in cui incidono, a partire da quelli che toccano sicurezza,

persone, risorse finanziarie e comunicazioni esterne.

## 4.2 I PROTOCOLLI DI CONTROLLO

Appare inoltre opportuno integrare i presidi in una **parte speciale dedicata**, raccordata con il sistema di gestione dei rischi previsto dall'AI Act e, ove adottato, con un sistema di gestione dell'IA conforme allo *standard* ISO/IEC 42001 (la cui certificazione potrebbe costituire un indice, ma non certo una presunzione, di idoneità del Modello). Potrebbero essere utilmente proceduralizzati, in particolare:

- l'**approvazione all'uso** dei sistemi, con individuazione del *process owner* e del responsabile della decisione che l'IA influenza;
- la **sorveglianza umana effettiva**, con individuazione nominativa dei soggetti incaricati, formazione adeguata, poteri reali di intervento e di arresto del sistema e tempi di reazione compatibili con la sua dinamica (una firma a valle non è vera sorveglianza se chi firma non comprende i limiti del sistema o non può dissentire);
- il **change management**, con nuova validazione in caso di modifiche a modelli, dati o configurazioni;
- la **gestione degli incidenti** e delle anomalie, con i connessi obblighi di segnalazione alle autorità;
- il **presidio contrattuale verso i fornitori**, con clausole di *audit*, flussi informativi, livelli di servizio

in materia di sicurezza e ripartizione documentata dei ruoli;

- i **presidi di cybersicurezza** (segregazione degli accessi ai modelli, integrità dei *dataset*, tracciabilità degli interventi), che costituiscono al tempo stesso misure di sicurezza informatica e cautele rilevanti ai sensi dell'art. 437-bis c.p.;
- per il rischio *deepfake*, procedure di **verifica del consenso, della provenienza e dell'approvazione** dei contenuti sintetici prima della loro diffusione.

Il sistema disciplinare dovrebbe essere esteso alle violazioni delle procedure in materia di IA, e i canali di *whistleblowing* (D.Lgs. 24/2023) potrebbero espressamente contemplare le segnalazioni relative a malfunzionamenti, alterazioni e carenze della sorveglianza umana. Resta inteso che l'efficacia di tali presidi potrà essere apprezzata soltanto alla prova dei fatti: la giurisprudenza, come noto, richiede la verifica in concreto dell'effettività del Modello, e non la mera esistenza documentale delle procedure.

## 4.3 LA DOCUMENTAZIONE COME PRESIDIO

Nella materia in esame, la documentazione tecnica (registri degli eventi, esiti dei *test*, documentazione del sistema di gestione dei rischi, parametri della supervisione umana) è insieme adempimento regolatorio, prova dell'idoneità del Modello,

materiale probatorio sul pericolo concreto e parametro di commisurazione della sanzione.

Lo conferma, sul versante civilistico, lo stesso D.Lgs. n. 160/2026, che consente al giudice di ordinare l'**esibizione** di tali elementi nelle azioni di risarcimento dei danni cagionati da sistemi di IA (art. 17), presume il **nesso di causalità** quando il danno derivi dalla violazione di obblighi dell'AI Act (art. 18) e precisa che la conformità del sistema, anche se certificata, **non esclude di per sé la responsabilità** (art. 19). Il principio operativo che sembra potersene trarre è il seguente: la documentazione va progettata insieme al controllo, non ricostruita dopo un incidente.

#### 4.4 IL RUOLO DELL'ORGANISMO DI VIGILANZA E LA CATENA DELLE RESPONSABILITÀ

Il presidio del rischio IA è strutturalmente **policentrico**: coinvolge, tra gli altri, la funzione legale, la *compliance*, il CFO, le funzioni IT e il CISO, il DPO, le funzioni operative e l'RSPP. Il Modello dovrà disegnare con chiarezza le interfacce tra tali funzioni, evitando sovrapposizioni e zone grigie.

All'**Organismo di Vigilanza** spetterà la vigilanza di secondo livello sull'effettivo funzionamento del sistema, senza trasformarsi in gestore dell'IA. A tal fine, appare opportuno:

- integrarne le competenze tecnologiche, quantomeno mediante il ricorso stabile a consulenti esperti;

- prevedere **flussi informativi dedicati** (esiti dei test e delle valutazioni di conformità, *incident report*, deroghe alla sorveglianza umana, modifiche sostanziali ai sistemi, esiti degli *audit* sui fornitori), con soglie di *escalation* predefinite;
- svolgere verifiche a campione sull'effettiva operatività dei presidi.

#### 4.5 LE CONDOTTE RIPARATORIE

Infine, il sistema 231 offre anche rispetto ai nuovi illeciti i consueti strumenti premiali, la cui valorizzazione merita di essere pianificata *ex ante*. Gli artt. 12 e 17 del Decreto 231 consentono, rispettivamente, la riduzione della sanzione pecuniaria e l'esclusione delle sanzioni interdittive qualora l'ente, prima dell'apertura del dibattimento, abbia eliminato le conseguenze del reato, adottato un Modello idoneo e messo a disposizione il profitto conseguito.

Trasposto all'art. 437-*bis* c.p., ciò potrebbe essere integrato da: sospensione del sistema pericoloso, *remediation* tecnica documentata, adozione o revisione della parte speciale dedicata all'IA e quantificazione del risparmio di spesa conseguito. La natura di reato di pericolo potrebbe giocare qui, per una volta, a favore dell'ente: l'eliminazione delle conseguenze pericolose appare, almeno in astratto, tecnicamente possibile in modo pieno (il sistema si disattiva, si corregge, si ri-valida), a

differenza di quanto accade per gli eventi lesivi irreversibili.

## 5. CONCLUSIONI

L'art. 437-*bis* c.p. segna l'ingresso del rischio tecnologico da intelligenza artificiale nel diritto penale d'impresa e il nuovo art. 25-*vicies* ne costituisce il naturale completamento sul versante dell'ente.

Il modello prescelto – reato di pericolo concreto, eterointegrato da una disciplina cautelare di matrice europea, punibile anche a titolo di colpa grave – sembra riproporre, amplificandole, le tensioni già note alla materia prevenzionistica: l'interesse o vantaggio potrebbe trovare nel risparmio sui costi della sicurezza tecnologica un terreno elettivo, mentre la colpa di organizzazione potrebbe assumere la fisionomia inedita del **difetto di governo di un agente semi-autonomo**.

Per le imprese, l'indicazione più ragionevole sembra essere la seguente: l'intelligenza artificiale non può essere trattata come un capitolo aggiuntivo del Modello, ma come una **dimensione trasversale dell'intero risk assessment**. Il passaggio, ancora una volta, è dall'algoritmo all'organizzazione: le nuove regole non puniscono condotte *"della macchina"* né eliminano la responsabilità umana, ma spingono le imprese a renderla **chiara, attribuita e dimostrabile nel tempo**.

Molto, tuttavia, resta ancora da chiarire. Sarà l'esperienza applicativa – e, in particolare, l'elaborazione giurisprudenziale sui primi casi concreti – a dire se le nuove fattispecie troveranno effettiva applicazione e quali presidi organizzativi saranno ritenuti idonei a fondare l'esonero dell'ente. Nell'attesa, un approccio prudente e proporzionato al rischio sembra la scelta più ragionevole.

# CONTATTI



**Giuseppe Fornari**  
Founding Partner

[g.fornari@fornarieassociati.com](mailto:g.fornari@fornarieassociati.com)



**Martina Pangallo**  
Associate

[m.pangallo@fornarieassociati.com](mailto:m.pangallo@fornarieassociati.com)



**Pietro Frazzica**  
Associate

[p.frazzica@fornarieassociati.com](mailto:p.frazzica@fornarieassociati.com)

## **Milano**

Via Chiossetto 18

T: +39 0254122206

E:

[milano@fornarieassociati.com](mailto:milano@fornarieassociati.com)

## **Roma**

Piazza Adriana 5

T: +39 0622201000

E: [roma@fornarieassociati.com](mailto:roma@fornarieassociati.com)

## **Bari**

Via Principe Amedeo 25

T: +39 080 918 4280

E: [bari@fornarieassociati.com](mailto:bari@fornarieassociati.com)

Questa pubblicazione ha lo scopo di fornire informazioni di carattere generale rispetto all'argomento trattato e non deve quindi essere considerata come un parere legale né come una disamina esaustiva di ogni aspetto relativo alla materia oggetto del documento.

**Fornari e Associati**  
**[www.fornarieassociati.com](http://www.fornarieassociati.com)**